De bescherming van persoonsgegevens

Berkvens, J.M.A.; Prins, J.E.J.

Published in:
Recht en computer

Publication date:
2014

Document Version
Peer reviewed version

De bescherming van persoonsgegevens

J.M.A. Berkvens[1]*, J.E.J. Prins*[2]

1. Inleiding

Het onderwerp van dit hoofdstuk heeft de afgelopen jaren een stormachtige ontwikkeling doorgemaakt. En alhoewel beide onderwerpen vaak in een adem worden genoemd, gaat het bij de bescherming van persoonsgegevens bovendien om een (overigens steeds belangrijker) deelaspect van het bredere onderwerp 'privacybescherming'. Nu zelfs een summiere bespreking van alle – voor beide onderwerpen – relevante aspecten, niet past binnen de voor dit hoofdstuk beschikbare ruimte, is ervoor gekozen de onderstaande bespreking te beperken tot de kaderwet voor de bescherming van persoonsgegevens: de Wet bescherming persoonsgegevens (Wbp) en de aanstaande actualisering hiervan. De Wbp strekt tot implementatie van de Europese richtlijn 95/46/EG. Wij bespreken in het onderstaande de belangrijkste elementen uit deze wet alsmede de ontwikkelingen in jurisprudentie, beleid en literatuur die de afgelopen aan deze elementen een nadere invulling hebben gegeven. Voor het overige verwijzen wij naar beschikbare handboeken, dissertaties, de ruime voorraad tijdschriftartikelen en vele toelichtingen op wettelijke regelingen (zoals de informatie op de website van het College Bescherming Persoonsgegevens – Cbp).

2. De Wet bescherming persoonsgegevens

Reikwijdte Wbp en definities

Reikwijdte

De reikwijdte van de Wbp wordt bepaald door de begrippen 'persoonsgegeven' en 'verwerken'. Het object van de regelgeving is namelijk het *verwerken* van *persoonsgegevens*. De Wbp definieert een persoonsgegeven als elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Daarbij moet het gaan om levende personen.[3] Gegevens betreffende kleine ondernemingen worden geacht persoonsgegevens van de ondernemer te zijn.[4] Er moet dus aan twee vereisten worden voldaan. Op de eerste plaats dient er sprake te zijn van gegevens die betrekking hebben op een natuurlijke persoon. Op de tweede plaats dient het te gaan om een identificeerbare of geïdentificeerde persoon.[5]

Of gegevens informatie over een persoon verschaffen zal vaak op het eerste gezicht duidelijk zijn. Ook is denkbaar dat gegevens niet primair betrekking hebben op personen doch op bijvoorbeeld goederen, gebeurtenissen, gedachten. Indien dergelijke gegevens tevens informatie kunnen bevatten die betrekking heeft op personen dienen zij blijkens de memorie van toelichting toch als persoonsgegevens te worden beschouwd.[6] Objectgegevens dienen in beginsel niet als een persoonsgegeven te worden beschouwd.[7] Indien echter een reële mogelijkheid bestaat dat een verband met een persoon gelegd kan worden (een theoretische mogelijkheid daartoe is niet voldoende), dan kan er toch sprake zijn van een persoonsgegeven.[8] Zo is vele jaren geleden al door de Registratiekamer vastgesteld dat gegevens over transacties en verkoopprijzen van woningen en kentekens van auto's persoonsgegevens zijn, omdat deze gegevens informatie over een bepaald persoon kunnen verschaffen.[9] Ook zullen de op het internet gebruikte IP-nummers in veel gevallen als persoonsgegevens moeten worden aangemerkt.[10]

---

[1] Adjunct directeur Juridische Zaken bij Rabobank Nederland en em. hoogleraar Informatica en Recht (Radboud Universiteit Nijmegen).

[2] Hoogleraar recht en informatisering, Universiteit van Tilburg, decaan Juridische Faculteit.

[3] Voorzover gegevens betreffende een overledene ook informatie kunnen verschaffen over levende personen kunnen ze onder omstandigheden toch als persoonsgegeven gelden (*Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 50).

[4] *Kamerstukken II*, 1997/98, 25 892, nr. 3, blz. 47.

[5] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 45-46.

[6] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 46-47.

[7] Europees hof voor de rechten van de mens (vierde kamer), 4 januari 2007, nr. 39658/05, *RvdW* 2007, 449 (onderscheid zaaksgegevens versus persoonsgegevens).

[8] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 47.

[9] Registratiekamer, 29 december 1994, 94.E.064 en Registratiekamer 15 oktober 1993, 92.F.008.

[10] G.J. Zwenne, *De verwaterde Privacywet* (oratie: Leiden RUL), Leiden: april 2013.

Het is niet voldoende dat gegevens betrekking hebben op een persoon. Het moet gaan om een identificeerbare persoon. De identiteit moet redelijkerwijs zonder onevenredige inspanning kunnen worden vastgesteld.[11] Indien geen feitelijke mogelijkheden voor de verantwoordelijke aanwezig zijn om gegevens die betrekking hebben op *personen* in relatie te brengen tot *bepaalde personen* is er geen sprake van persoonsgegevens.[12] De afgelopen jaren heeft de Artikel 29-Werkgroep van de Europese Commissie meerdere adviezen gepubliceerd die relevant zijn voor de interpretatie van het begrip persoonsgegeven. We noemen hiervan: Advies 4/2007 van 20 juni 2007; Advies 1/2008 van 4 april 2008 en Opinie 13/2011 van 16 mei 2011.[13] Uit een analyse van de verschillende opinies wordt duidelijk dat aan het begrip een steeds ruimere uitleg wordt gegeven.[14]

Als gegevens afdoende geanonimiseerd zijn is er geen sprake meer van persoonsgegevens. Toch is anonimisering niet altijd voldoende omdat niet valt uit te sluiten dat door spontane herkenning herleiding mogelijk wordt. Onder spontane herkenning wordt de mogelijkheid verstaan dat geanonimiseerde gegevens door toevallige factoren met een bepaalde persoon in verband kunnen worden gebracht. Indien de mogelijkheid van spontane herkenning redelijkerwijs is uitgesloten gelden geanonimiseerde gegevens niet meer als persoonsgegevens.[15] Bij deze benadering kan de kanttekening worden geplaatst dat het merkwaardig is dat ook gegevens waarvan achteraf kan worden vastgesteld dat nooit herleiding heeft plaatsgevonden toch vanwege het theoretische herkenningsrisico aan privacyregels onderworpen zijn geweest. Overigens geldt voor gegevens die de facto herleid worden dat ze automatisch gaan vallen in het beschermingsregime voor persoonsgegevens hetgeen leidt tot de verplichting voor de verantwoordelijke om alle herkende personen te informeren dat hun gegevens bijvoorbeeld in het kader van onderzoeksdoeleinden worden verwerkt.

De vraag of al dan niet sprake is van een persoonsgegeven is van belang voor de status van profilerings- en datamining-technieken onder de Wbp. Middels dergelijke technieken kunnen groepsprofielen worden verkregen die eigenschappen van groepen van mensen weergeven in termen van prognoses (bijvoorbeeld inzake gezondheid, criminaliteit, enzovoort), gedrag (bijvoorbeeld koopgedrag of wanbetalers), significante verschillen met andere groepen, enzovoort. Deze profielen worden aangemaakt op basis van vele gegevens, waaronder veel persoonsgegevens. Aan de hand van de verkregen profielen kunnen consumenten, burgers en andere hoedanigheden waarin personen in het maatschappelijk verkeer participeren in een bepaalde categorie worden geplaatst op basis waarvan selectie en uitsluiting van individuele personen plaatsvindt: hen wordt al dan niet een aanbieding gedaan, een verzekering verstrekt, een overheidsvoorziening aangeboden, enzovoort.[16] De belangrijke vraag bij de toepassing van dergelijke technieken is in hoeverre er tijdens de diverse stadia van datamining gebruik wordt gemaakt van persoonsgegevens. Veelal zal er immers een zodanige mate van anonimisering hebben plaatsgevonden, dat de gegevens helemaal niet, of niet zonder een onevenredige inspanning herleid kunnen worden tot een individu.[17] De profielen en indicatoren als zodanig zijn derhalve niet als persoonsgegeven aan te merken.[18] De potentieel privacybedreigende factor is echter gelegen in het feit dat de profielen worden toegepast *alsof* ze een persoonsgegeven zijn.[19] Probleem is vervolgens dat als een burger of consument door het gebruik van een bepaald profiel wordt benadeeld, hij of zij geen beroep kan doen op de Wbp.[20] Kenmerkend hierbij is dat weliswaar gegevens worden gehanteerd die niet in strikte zin als persoonsgegevens kunnen worden aangemerkt, maar die in eerste instantie wel aan individuele personen zijn onttrokken en die, na aggregatie, bewerking en eventuele verrijking met andere gegevens, worden gebruikt om tot beoordeling en beleidsvorming ten aanzien van (leden van) categorieën van personen te komen. In de kabinetsbrief van 29 april 2011 kondigde het vorige kabinet aan in de toekomst te komen met: "Een afzonderlijke regeling met specifieke transparantieverplichtingen bij het toepassen

---

[11] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p.47.

[12] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 50-52. Zie ook: Rb. Amsterdam 16 februari 2012, *LJN* BV6122, *Computerrecht* 2012/122, m.nt. F. van der Jagt.

[13] Alle beschikbaar via de website van de Werkgroep: http://ec.europe.eu/justice/policies/privacy/docs/wpdocs.

[14] Colette Cuijpers, Paul Marcelis, "Oprekking van het concept persoonsgegevens beperking van privacybescherming?", *Computerrecht* afl. 6 2012, pp. 397-409.

[15] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 48.

[16] Zie nader over deze techniek en de mogelijkheden de diverse hoofdstukken in: Mireille Hildebrandt, Serge Gutwirth (eds), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Springer2008.

[17] Waarbij overigens moet worden opgemerkt dat bij het proces van anonimiseren de regels van de Wbp van toepassing kunnen zijn omdat de gegevens alvorens ze zijn geanonimiseerd wel als persoonsgegeven aangemerkt moeten worden.

[18] Tenzij ze worden vastgelegd als persoonsgegeven bij de andere gegevens van de betreffende persoon.

[19] Het College Bescherming Persoonsgegevens lijkt al snel een voor de Wbp relevante situatie aanwezig te achten. Zie hoofdstuk 5 uit *De gewaardeerde klant*, serie A&V, nr. 18.

[20] Zulks tenzij het profiel wordt gebruikt in een geautomatiseerd procédé waarbij als onderdeel van het proces het profiel wordt toegepast op persoonsgegevens van de betrokkene. In dat geval kan de betrokkene een beroep doen op art. 42 Wbp.

van profileringen, met inbegrip van een explicitering van het doel van de verwerking, en de daarbij gehanteerde categoriseringen".[21]

De Wbp is van toepassing op *verwerkingen* van persoonsgegevens. Het begrip verwerking heeft een zeer ruime strekking. Het omvat iedere mogelijke technische verwerkingshandeling of gebruikshandeling met betrekking tot een persoonsgegeven. Dat betekent dat iedere handeling vanaf de verzameling en opslag tot de verwijdering en vernietiging van een persoonsgegeven als een verwerkingshandeling dient te worden opgevat.[22] In de gehanteerde ruime definitie worden primaire handelingen en secundaire handelingen gelijkgeschakeld.[23] Onder primaire handelingen verstaan wij het gebruik van de persoonsgegevens door de verwerker voor het beoogde doel en de overdracht door de verwerker van het gebruiksrecht van de gegevens aan een derde. Onder secundaire handelingen verstaan wij de louter technische handelingen die strekken tot ondersteuning van [accessoir zijn aan] de primaire handelingen. Het gaat daarbij om het verzamelen, opslaan, transporteren, bewerken van gegevens. Het begrip verwerking wordt enerzijds gehanteerd in de enkelvoudige betekenis waarbij het gaat om afzonderlijke handelingen. Anderzijds wordt het begrip verwerking gebruikt om een *samenhangend geheel* van handelingen aan te duiden. Het achtereenvolgens ontvangen van een brief met persoonsgegevens, het kennis nemen van de inhoud, het archiveren in een bestand of het inscannen en elektronisch archiveren, het verwijderen en vernietigen van de persoonsgegevens kan dus ook als één verwerking worden bestempeld. De betekenis van de begrippen verstrekken en verzamelen wordt naar aanleiding van opmerkingen van de Raad van State nog in aparte onderdelen van art. 1 Wbp nader uitgelegd.

De mogelijke relevantie van een verwerking in de context van de bescherming van de persoonlijke levenssfeer doet weinig terzake. Ook technische verwerkingshandelingen betreffende persoonsgegevens die geen persoonsgerichte context hebben worden getroffen door de Wbp.[24] Wel is van belang dat degene die de verwerkingshandeling voor zijn rekening neemt enige feitelijke macht over de persoonsgegevens kan uitoefenen (niet relevant is of deze invloed daadwerkelijk wordt uitgeoefend). Van feitelijke macht zal daarom al snel sprake zijn.[25] Ter illustratie citeren we uit de tekst van de memorie van toelichting bij art. 1 Wbp: 'Een telecomoperator die enkel gegevens doorvoert zonder daarop enige invloed uit te kunnen oefenen, verwerkt daarmee geen persoonsgegevens. Wanneer echter bijvoorbeeld een Internet service provider de mogelijkheid heeft het verspreiden van onrechtmatige berichten tegen te gaan, is er wel sprake van mogelijke invloed en daarmee van gegevensverwerking en is daarom de wet volledig van toepassing'.

De Wbp is van toepassing indien sprake is van een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens. Indien dus sprake is van een aantal opeenvolgende geautomatiseerde handelingen in combinatie met niet-geautomatiseerde handelingen, zal het geheel van handelingen als één *gedeeltelijk geautomatiseerde* verwerking kunnen worden aangemerkt en door de Wbp worden bestreken. De term 'geheel' is dus van cruciale betekenis. De toelichting geeft weinig informatie. Hoe zit het bijvoorbeeld als een verwerkingsproces achtereenvolgens via een keten van verschillende 'verantwoordelijken' loopt? De vraag wordt dus hoe de praktijk hier in de toekomst mee uit de voeten kan. Tevens is de wet van toepassing indien sprake is van een niet-geautomatiseerde verwerking van persoonsgegevens die in een *bestand* zijn opgenomen of bestemd zijn om daar in te worden opgenomen. Daarbij wordt gedoeld op al dan niet langs geautomatiseerde weg gevoerde *verzamelingen* van persoonsgegevens. Tijdens de voorbereiding van de Wbp is discussie gevoerd over de wenselijkheid om ook enkelvoudige dossiers onder het bereik van de Wbp te brengen. Men heeft evenwel besloten om de toelichting op de richtlijn te volgen (considerans (27)). Er moet derhalve worden aangenomen dat het bestandsbegrip in de Wbp slechts geldt voor bestanden die op meer dan één persoon betrekking hebben.[26]

De omschrijving van het begrip bestand lijkt overigens voor de praktijk van weinig betekenis. Geautomatiseerde bestanden, of het nu gaat om één of meer elektronische dossiers die op één of meer personen betrekking hebben, vallen per definitie reeds onder de Wbp.[27] Voorts zijn de grenzen tussen de gedeeltelijk geautomatiseerde verwerking en de niet-geautomatiseerde verwerking van gegevens die in een bestand zijn of worden opgenomen

---

[21] *Kamerstukken II*, 2010/11, 32761, nr. 1.

[22] De enkelvoudige transmissie van gegevens vormt blijkens de memorie van toelichting op p. 52 en memorie van toelichting op p. 60 een uitzondering. Vergelijk ook art. 4 lid 2 inzake de doorvoer van persoonsgegevens.

[23] Een beperkte uitzondering geldt wellicht voor sommige hulpmiddelen als back-upbestanden zij het dat de reikwijdte van deze uitzondering beperkter is dan onder de WPR. Vergelijk de memorie van toelichting op p. 54.

[24] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p.51.

[25] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 51-52.

[26] Rb. Utrecht 17 november 2010, *LJN* BO5230. Zie ook het zogenaamde Zwartboek arrest: HR 3 juni 2005, *LJN* AT1093.

[27] Zie echter: ECLI:NL:RBROT:2013:6686. Wbp niet van toepassing op documenten in 'intern record management' systeem.

betrekkelijk vaag. Als het de bedoeling is dat geautomatiseerd verwerkte gegevens in een handmatig bestand worden opgenomen geldt de Wbp op basis van het eerste criterium (geheel of gedeeltelijk geautomatiseerde verwerking) ook voor de gegevens in het bestand.[28] Ook indien het bestand een enkelvoudig dossier is dat buiten de wettelijke definitie van een bestand valt. Voorts kan sprake zijn van een op zich ongestructureerde dossierverzameling. Zodra er sprake is van een mogelijkheid om een dergelijke verzameling met behulp van enige vorm van automatisering te ontsluiten is er toch sprake van een gestructureerd bestand waarbij de structuur door de parallelle vorm van automatisering wordt gevormd.[29]

Uitzonderingen

Diverse wettelijke regelingen kennen deels van de Wbp afwijkende regimes voor de verwerking van persoonsgegevens. In artikel 2 van de Wbp worden verwerkingen die onder daar genoemde wetgeving vallen *geheel* vrijgesteld van de Wbp. Naast deze vrijstellingen worden op grond van dit art. 2 ook verwerkingen van persoonsgegevens voor persoonlijk gebruik vrijgesteld. Wat daaronder valt staat te lezen in de memorie van toelichting op de Wbp: *Het «persoonlijk gebruik» ziet zowel op de situatie buiten het werk als daarbinnen. Veel beroepsbeoefenaars houden (…), ook in het kader van hun werk, eigen lijstjes bij, bijvoorbeeld adresbestanden van personen met wie zij regelmatig contact onderhouden. Zij hebben het karakter van persoonlijke aantekeningen, dienend als geheugensteun. Deze laatste zijn van de werking van het wetsvoorstel uitgezonderd. Dit wordt niet anders wanneer bij voorbeeld een secretaresse van de beroepsbeoefenaar in bijzondere gevallen ook daarvan kennis neemt.*[30] *Zodra echter een verwerking beoogd is voor gebruik door meerdere personen, is het wetsvoorstel van toepassing.* In de Dexiazaken kwam de reikwijdte van art. 2 lid 2 sub a eveneens aan de orde waar de Hoge Raad in RO 3.14 het volgende opmerkt: *Het hof heeft voornoemde notities terecht onderscheiden van interne notities die de persoonlijke gedachten van medewerkers van Dexia bevatten en die uitsluitend zijn bedoeld voor intern overleg en beraad, omdat het bij laatstgenoemde notities veel minder vanzelfsprekend is dat deze bedoeld zijn om tezamen met andere persoonsgegevens in een bestand te worden opgenomen.*[31]

Journalistiek

De oorspronkelijke vrijstelling voor persoonsregistraties uitsluitend ten dienste van openbare informatievoorziening via pers, radio of televisie alsmede die voor boeken en andere schriftelijke publicaties is vervangen in art. 3 door een beperkte uitzondering voor verwerkingen uitsluitend voor journalistieke, artistieke of literaire doeleinden.[32]

De verantwoordelijke

De Wbp richt zich primair tot de verantwoordelijke. Ten aanzien van iedere verwerking van persoonsgegevens kan er een verantwoordelijke worden aangewezen. Bij het bepalen wie als verantwoordelijke moet worden aangemerkt wordt gekeken wie doel en middelen van een verwerking vaststelt. Het gaat daarbij om de vraag wie bepaalt of er gegevens worden bewerkt, welke gegevens er worden bewerkt, welke bewerking wordt toegepast en op welke wijze dat gebeurt en voor welk doel.[33] In Opinie heeft de Werkgroep-29 van de Europese Commissie een nadere uitwerking gegeven van het begrip en de diverse criteria toegelicht aan de hand van diverse praktijkvoorbeelden.[34]

De Wbp kijkt naar de zeggenschap over de verwerking. Binnen de overheid ligt die bij het relevante bestuursorgaan in de zin van de Algemene wet bestuursrecht. Binnen de particuliere sector is dat veelal een rechtspersoon. Een specifieke situatie geldt hier bij concernverhoudingen, waar niet steeds eenvoudig zal zijn vast te stellen wie als verantwoordelijke voor een verzameling van verwerkingen moet worden aangemerkt. Om duidelijkheid te bieden is de figuur van de concernverantwoordelijke erkend.[35] Criterium is of uit statuten of overeenkomsten kan worden afgeleid dat de holding als verantwoordelijke voor verwerkingen binnen het concern mag worden aangemerkt.[36]

---

[28] Tenzij het begrip verwerking eindigt na de laatste geautomatiseerde stap!

[29] Zie p. 96 van de eerste druk van dit boek.

[30] Zie *Kamerstukken II*, 1997/98, 25 892, nr. 3, blz. 70.

[31] HR 29 juni 2007,*LJN* AZ4663 en HR 29 juni 2007 *LJN* AZ4664.

[32] In de CBP Richtsnoeren publicatie van persoonsgegevens op internet, Stcrt 11 december 2007, p. 42 wordt ingegaan op de journalistieke exceptie.

[33] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 55.

[34] Artikel 29-Werkgroep van de Europese Commissie, *Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker'*, Brussel 16 februari 2010.

[35] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 56.

[36] Voor een kritische beschouwing over de relatie tussen Wbp en vennootschapsrecht zij verwezen naar de dissertatie van M.B.J. Thijssen,

Waar in het verleden een natuurlijk persoon slechts in een enkel geval als verantwoordelijke kon worden aangemerkt (te denken viel toen aan een eenmanszaak), verwerken met de intrede en populariteit van online sociale netwerken - Facebook, LinkedIn en YouTube - ook zij steeds vaker persoonsgegevens waarmee ze als verantwoordelijke zijn aan te merken.[37] Volgens de rechtbank Den Bosch is de beheerder van de website een verantwoordelijke omdat deze gegevens aanvult en deze gegevens toegankelijk maakt door middel van een emailservice.[38]

Een bijzonder aandachtspunt vormt het gegeven dat bij verwerkingsprocessen vaak sprake zal zijn van meer dan één belanghebbende bij een verwerking. Indien dat binnen een enkel bestuursorgaan of rechtspersoon is levert dit geen problemen op: er blijft uiteindelijk slechts één enkele verantwoordelijke. Indien echter meer dan één bestuursorgaan of rechtspersoon belanghebbende wordt kan sprake zijn van een samengestelde verantwoordelijkheid. Dat het desalniettemin lang niet altijd eenvoudig is om vast te stellen welk type verantwoordelijkheid het betreft en wie dan exact de verantwoordelijke(n) is (zijn), toont het voorbeeld van cloud-diensten. De intrede deze diensten brengt onder meer onzekerheid met zich mee waar het gaat om het vaststellen van de verantwoordelijke voor de verwerking van persoonsgegevens 'in de wolk'.[39] De complexe relaties tussen verschillende betrokkenen en hun status onder de Wbp speelt ook bij de verwerking van persoonsgegevens via smartphones en de daarop geplaatste apps.[40] Zo zijn bij de ontwikkeling, distributie en de toepassing van apps partijen betrokken als app-ontwikkelaars, app stores, advertentiebedrijven en leveranciers van besturingssystemen. Via apps worden grote hoeveelheden persoonsgegevens verwerkt en gecombineerd. Gemiddeld blijkt iedere smartphone-gebruiker zo'n 37 apps te hebben gedownload. In het voorjaar 2013 publiceerde de Werkgroep-29 van de Europese Commissie Opinie 02/2013 waarin rechten en plichten van alle betrokkenen uiteen worden gezet en voor de praktijk relevante handvaten voor de toepassing van de verplichtingen worden geboden.

Bewerker

Bij de vraag wie als verantwoordelijke dient te worden aangemerkt komt ook de figuur van de bewerker in beeld. Het gaat daarbij om situaties waarin de verantwoordelijke een verwerking heeft uitbesteed aan een derde. De Wbp spreekt over de bewerker als degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt zonder aan zijn rechtstreeks gezag te zijn onderworpen. Deze definitie is niet zo eenvoudig als op het eerste oog lijkt. De toelichting geeft aan dat kenmerkend voor de bewerker is dat hij geen zeggenschap heeft over doel en middelen voor de verwerking. Hij neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens.[41] Het verwerken van de gegevens als zodanig vormt een hoofdtaak. Indien er sprake is van een verwerking die voortvloeit uit een andere vorm van dienstverlening dient de betrokkene toch als verantwoordelijke te worden aangemerkt.[42] De toelichting geeft onder meer als voorbeeld een advocaat. Toch kan op grond van de criteria worden volgehouden dat een advocaat in de rol van de bewerker zit. Het is immers zijn opdrachtgever die bepaalt of een dossier in behandeling wordt genomen. Het is ook de opdrachtgever die bepaalt of een zaak wordt doorgezet en of het toegelaten is dat bepaalde gegevens aan derden worden verstrekt. Ook het voorbeeld van een telemarketingbedrijf dat als verantwoordelijke wordt aangemerkt als het voor derden een onderzoek verricht kan langs de lijn van de toelichting als bewerker worden aangemerkt. Uit het enkele feit dat de opdrachtnemer zelf gegevens omtrent de opdracht vastlegt kan naar onze mening evenmin worden afgeleid dat hij als verantwoordelijke moet worden aangemerkt.[43] Het betreft immers gegevens die hij nodig heeft om te kunnen factureren of om verantwoording voor zijn werkzaamheden af te leggen. Ten aanzien van die gegevens is hij uiteraard wel als verantwoordelijke aan te merken.

De grenzen tussen verantwoordelijke en bewerker zijn niet altijd goed vast te stellen.[44] Dit bleek in het verleden al bij de zogenaamde Swift-case, waar de Amerikaanse autoriteiten een back up bestand van Swift onderzochten.[45]

De Wbp en de vennootschap, Serie Recht en Praktijk 171, Kluwer Deventer, 2009.

[37] Zie ook het Advies 5/2009 van 12 juni 2009 van de Werkgroep-29 van de Europese Commissie over online sociale netwerken.

[38] Rb. Den Bosch 31 januari 2013, *LJN* BZ2126.

[39] Zie de zienswijze van het College Bescherming Persoonsgegevens van 10 september 2012 over cloud-diensten (beschikbaar via www.cbpweb.nl).

[40] Zie ook: E. Valgaeren, L. Leitner, "Smartphones en privacy. Vrienden, vijanden of ergens tussenin?", Computerrecht 2012/2.

[41] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 61.

[42] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 62.

[43] Een andere vraag die men zich kan stellen is of er wel behoefte bestaat aan het definiëren van een figuur als de bewerker. Het handelen van de bewerker wordt immers aan de verantwoordelijke toegerekend. Die wordt uitvoerig gereguleerd in de Wbp.

[44] WP 169, *Opinion 1/2010 on the concepts 'controller' and 'processor'*.

Indien men bijvoorbeeld kijkt naar de afwikkeling van een betaalopdracht valt op dat zowel de opdrachtgever, de bank van de opdrachtgever, de bank van de begunstigde, de tussenliggende verwerkingscentra en de begunstigde kunnen optreden als verantwoordelijke. Maar de partijen die betrokken zijn bij de afhandeling treden ook op in de rol van bewerker.[46] De Advocaat Generaal concludeerde in een zaak waarbij Google betrokken was dat de aanbieder van een zoekmachine niet noodzakelijkerwijze als verantwoordelijke dient te worden aangemerkt.[47]

Materiële normen en verwerkingsgronden

Algemeen

In art. 6 en 7 van de Wbp worden de algemene eisen geformuleerd voor de verwerking van persoonsgegevens: gegevens dienen in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze te worden verwerkt. Ze mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Daarbij dienen de gegevens toereikend, terzake dienend, niet bovenmatig, juist en nauwkeurig te zijn. Concreet betekenen deze eisen in de praktijk dat verwerkers onder meer de nodige aandacht moeten besteden aan het onderhoud van hun gegevensbestanden en – gegeven hetgeen met de verwerking wordt beoogd – kritisch moeten bezien welke gegevens nu precies noodzakelijk zijn. Dat betekent ook dat scherp in de gaten gehouden zal moeten worden hoe lang de gegevens bewaard mogen worden, ondanks dat de Wbp geen expliciete bewaartermijnen stelt.[48]

Het voornoemde stelsel van materiële normen wordt vervolgens in art. 8 Wbp aangescherpt door te stellen dat verwerking slechts is toegestaan indien *noodzakelijk* in verband met de in datzelfde art. 8 Wbp genoemde belangen dan wel met ondubbelzinnige toestemming van de betrokkene.[49] Bij het verzamelen van gegevens wordt dus niet slechts gekeken naar rechtmatigheids- en zorgvuldigheidsvoorwaarden. Het betreft achtereenvolgens de volgende gronden:

a. toestemming van de betrokkene;
b. ter uitvoering van een overeenkomst dan wel in het kader van het sluiten daarvan;
c. ter uitvoering van een wettelijke plicht;
d. bij een gevaar voor de gezondheid;
e. ter uitvoering van een publiekrechtelijke taak;[50]
f. bij een gerechtvaardigd belang van de verantwoordelijke of een derde.

In de praktijk zal de meerderheid van de gegevensverwerkende processen onder de gronden b t/m f geschaard kunnen worden. Het toestemmingsvereiste zal slechts in een beperkt aantal van de situaties de grondslag vormen. Als bijvoorbeeld wordt afgeweken van eerder met de betrokkene gemaakte afspraken. De Hoge Raad oordeelde dat bij ieder van de genoemde gronden het uitgangspunt van proportionaliteit en subsidiariteit in acht moet worden genomen.[51]

Het sluitstuk op de regeling wordt gevormd door art. 9 Wbp. Op grond van art. 9 mogen gegevens ook voor andere doeleinden worden verwerkt dan waarvoor ze zijn verzameld. Voorwaarde is dan dat het verdere verwerken niet onverenigbaar is met het oorspronkelijke verzameldoel. In alle situaties zal bij verstrekking gekeken moeten worden naar de verwantschap van de doelen. Er is hiermee gekozen voor een open toetsingskader, hetgeen betekent dat het antwoord op de vraag wat onder verenigbaar gebruik verstaan kan worden voor een belangrijk deel afhankelijk is van maatschappelijke opvattingen in plaats van juridische normen. Aanknopingspunten voor de beoordeling zijn onder meer: de aard van de gegevens, hetgeen gebruikelijk in de markt is, de gevolgen voor de

---

[45] Zie in meer detail: P. De Hert, B. de Schutter , "International transfers of data in the field of JHA: The lessons of Europol, PNR and Swift", pp. 299-335 in B. Martenczuk & S. van Thiel (eds.) *Justice, Liberty, Security: New challenges for EU external relations*. Brussels: VUB Press, 2008.

[46] J.M.A. Berkvens, 'Naar een wereld zonder controllers en processors', *P&I* 2011/5 p. 255.

[47] CONCLUSIE VAN ADVOCAAT-GENERAAL N. JÄÄSKINEN van 25 juni 2013 in Zaak C 131/12 (Google Spain).

[48] Zie hierover in meer detail: Bewaartermijnen van uw persoonsgegevens, College Bescherming Persoonsgegevens, Informatieblad 11a, Den Haag 2011.

[49] De term 'noodzakelijk' is tijdens de parlementaire behandeling van de Wbp voorwerp van discussie geweest. Het ging daarbij om de vraag of de vertaling van de Engelse term 'necessary' door 'nodig' beter zou zijn geweest. Blijkens de uitleg in de memorie van toelichting dient het begrip 'noodzakelijk' in horizontale relaties minder strikt te worden uitgelegd dan in verticale relaties. Vergelijk memorie van toelichting op p. 88.

[50] In het rapport *Werken met gegevens* Gegevensuitwisseling tussen CWI's en uitzendbureaus *Registratiekamer, juni 1999, 98.V.389* interpreteert de toenmalige Registratiekamer art. 8 sub e Wbp zodanig dat verstrekking door een uitzendbureau aan een bestuursorgaan op dat artikel kan worden gebaseerd. In andere gevallen vormt onderdeel f. een mogelijke basis. Zie p. 17. Zie ook HR 27 november 2012, *LJN* BY0215, R.O. 3.6.

[51] HR 9 september 2011, *LJN* BQ8097, *NJ* 2011, 595 m.nt. E.J. Dommering (Santander).

betrokkene en de wijze van verkrijging. Verder zal de verwerker passende waarborgen moeten nemen, zoals een voldoende informatieverstrekking aan de betrokkene over de verstrekking.[52] Voor de verdere verwerking gelden overigens ook de rechtvaardigingsgronden van art. 8 Wbp. De verenigbaarheidstoets van art. 9 kan in de gevallen genoemd in art. 43 Wbp achterwege blijven.

Bij de inkleuring van het toetsingskader speelt, met name voor de particuliere sector, de verplichte doelomschrijving van art. 7 Wbp een belangrijke rol. Veelal worden gegevens van klanten verzameld en verwerkt ten behoeve van een verzameling van activiteiten. Daarbij valt te denken aan het nakomen van contractuele verplichtingen. Gegevens worden uitgewisseld met toeleveranciers. Met financiële instellingen wordt het betalingsverkeer afgewikkeld. Soms vindt toetsing van kredietwaardigheid van de klant plaats. Gegevens worden verwerkt om de logistieke processen te optimaliseren, om frauderisico's te verkleinen. Ook worden gegevens gebruikt voor marktonderzoek en voor het benaderen van klanten. Ondernemingen die een verwerkingsdoel moeten omschrijven dienen zich dus ervan bewust te zijn dat het verwerkingsdoel al deze voorgenomen activiteiten dient te omvatten. Uiteraard staat het de ondernemer niet vrij om ongehinderd allerlei activiteiten in de doelomschrijving onder te brengen. Algemene rechtsbeginselen begrenzen zijn mogelijkheden. Klanten hoeven dus geen activiteiten te accepteren die in geen redelijke verhouding staan tot hun relatie met de ondernemer. Wordt de doelomschrijving te krap omschreven dan zal eerder met de verenigbaarheidstoets moeten worden gewerkt terwijl bij een adequate doelomschrijving een activiteit die binnen art. 8 is toegelaten gewoon is toegestaan. De doelomschrijving vindt voor wat betreft de Wbp haar begrenzing in de wettelijke eis dat er sprake moet zijn van een gerechtvaardigde doelomschrijving. De klant hoeft in het kader van een kooptransactie niet zomaar akkoord te gaan met allerlei nevenactiviteiten. Bij de vraag of direct marketing een geoorloofde activiteit is binnen de doelomschrijving betreffende de relatie tussen een verantwoordelijke en een betrokkene kan worden meegewogen dat art. 41 Wbp (naast art. 40 Wbp) reeds compenserende waarborgen bevat.[53]

Bijzondere gegevens

De Wbp kent een aangescherpt regime voor gevoelige gegevens, waarbij er nu wordt gesproken van bijzondere gegevens. Bij bijzondere gegevens gaat het om gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid[54], seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging. Ook worden strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag als gevoelig aangemerkt. [55] De hoofdregel van artikel 16 Wbp is dat de verwerking van deze gegevens verboden is. Per categorie van gevoelige gegevens worden uitzonderingen op deze hoofdregel geformuleerd in de artt. 17-22 Wbp. Verwerking van deze gegevens is tevens toegestaan indien sprake is van een zwaarwegend algemeen belang dan wel een dergelijke verwerking bij wet voorgeschreven is (zie art. 23 Wbp).

Toestemmingsvereiste

In de Wbp wordt in een aantal gevallen als vereiste gesteld dat de betrokkene toestemming heeft gegeven voor een bepaalde verwerking. De Wbp definieert toestemming als elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt. Er wordt geen geschriftsvereiste gesteld. Het begrip toestemming komt conform de definitie voor in art. 17 lid 3, 19 lid 2, 20 lid 2 en 79 (onder verwijzing naar art. 1 sub *i*) Wbp. Daarnaast wordt in enkele bepalingen gesproken over 'ondubbelzinnige' toestemming: art. 8 sub *a*, en 77 lid 1 sub *a* Wbp. Ook wordt op enkele plaatsen gesproken over 'uitdrukkelijke' toestemming: art. 23 lid 1 sub *a*, 23 lid 2 sub *c* Wbp. Wil de toestemming voldoen aan de eisen dan dient aan de volgende drie elementen te zijn voldaan: vrijheid van beslissen, duidelijke omschrijving van de reikwijdte van de toestemming en op basis van goede informatie.[56] In het geval ondubbelzinnige toestemming is vereist 'moet iedere twijfel zijn uitgesloten' bij de verantwoordelijke omtrent de toestemming. Doorgaans betekent dat een zwaardere informatieplicht richting betrokkene. Ook kan er sprake zijn van een verificatieplicht. In de toelichting wordt het uit handen geven van een smart card of het in een interactieve omgeving herhaald aanklikken van een ja-knop aangemerkt als een omstandigheid die verdere verificatie overbodig maakt.

---

[52] De desbetreffende tekst van art. 9 lid 2 is in eerste instantie uit het wetsvoorstel geschrapt maar naderhand weer teruggeplaatst.

[53] Zie J.M.A. Berkvens, 'Het goede doel', *Privacy en informatie* 2001, nr. 2, p. 64-69.

[54] Zie ook de Lindqvist zaak. De mededeling dat iemand zijn voet had gestoten werd door het Europese Hof als een gevoelig gegeven aangemerkt (Prejudiciële zaak C101/01 (Bodil Lindqvist): overwegingen 49 t/m 51).

[55] Over het begrip strafrechtelijk gegeven zie RO 4.4 in LJN: BH4720, Hoge Raad , 08/00898 d.d. 29-05-2009.

[56] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 65.

Indien uitdrukkelijke toestemming is vereist, dient er sprake te zijn van een expliciete wilsuiting. Dat kan in woord, geschrift of gedrag. Een voorbeeld van dat laatste is wederom het dubbel aanklikken van een ja-knop of het overhandigen van een smart card. In het rapport *Klant in het web* merkte de Registratiekamer hier het volgende over op: 'Er zijn providers die de potentiële abonnee bij de installatie van de software uitdrukkelijk wijzen op de van toepassing zijnde algemene voorwaarden. Hierbij kan deze de software pas installeren nadat hij door het aanklikken van een daartoe bestemde button verklaart kennis genomen te hebben met de getoonde algemene voorwaarden en zich akkoord verklaard met de daarin opgenomen voorwaarden. Voor zover de voorwaarden hierbij voldoen aan de inhoudelijke vereisten van ondubbelzinnige toestemming, is verdedigbaar dat de abonnee met die handeling inderdaad toestemming voor de gegevensverwerking verleent.'[57]

Een eenmaal gegeven toestemming kan blijkens de toelichting worden ingetrokken. De intrekking heeft geen terugwerkende kracht met betrekking tot verwerkingen in het verleden.[58] Voor zover de Wbp een zwaardere eis aan de aard van een toestemming stelt dienen de bestaande toestemmingsprocedures te worden aangepast. We wijzen in dit verband ook op art. 79 lid 2 Wbp.

Een illustratie van de consequenties die het toestemmingsvereiste met zich mee brengt, is te vinden is de eerder aangehaalde Opinie van de Werkgroep-29 over apps op smartphones. De ontwikkelaars van apps zullen: 1) toestemming moeten vragen voor de verwerking van persoonsgegevens voordat de app informatie van het apparaat haalt of daar informatie op plaatst, 2) afzonderlijk toestemming moeten vragen voor de verschillende soorten persoonsgegevens die de apps verwerkt, 3) duidelijke en begrijpelijke doelen aangeven waarvoor de gegevens worden gebruikt en deze doelen niet tussentijds wijzigen zonder toestemming, 4) gebruikers in de gelegenheid stellen hun toestemming in te trekken, de app te de-installeren en de al verzamelde persoonsgegevens te verwijderen.

Beveiliging en accountability

De verantwoordelijke dient er voor zorg te dragen dat de persoonsgegevens die onder zijn verantwoordelijkheid worden verwerkt zijn beveiligd tegen ongeautoriseerde toegang en verwerking. Begin 2013 publiceerde het College Bescherming Persoonsgegevens een geactualiseerde versie van de "Richtsnoeren beveiliging van persoonsgegevens" waarin een nadere uitwerking wordt gegeven van de algemene beveiligingsplicht zoals deze in art. 13 Wbp is neergelegd om "passende technische en organisatorische maatregelen" te nemen. Overigens betreft deze verplichting niet alleen de verwerking door de verantwoordelijke zelf maar ook de verwerking door voor de verantwoordelijke werkzame bewerkers.[59] Daarbij zorgt het fenomeen van cloud computing voor een extra dimensie aan de beveiligingsplicht.[60]

Een gerelateerd aandachtspunt is dat van de accountability. Dat betekent dan de verantwoordelijke niet alleen zich aan zijn wettelijke verplichtingen dient te houden maar dat hij bovendien binnen zijn organisatie toezicht organiseert op de naleving.[61] Onderdeel van een dergelijke toezichtsorganisatie kan een Functionaris voor de gegevensbescherming zijn. In sommige goedgekeurde privacygedragscodes is een verplichting opgenomen om het toezicht te organiseren.[62]

Rechten van betrokkenen

Algemeen

Welke rechten staan betrokkenen ter beschikking wanneer hun persoonsgegevens worden verwerkt? Naast kennisneming en correctie, wordt onder de Wbp aan degene van wie persoonsgegevens worden verwerkt een recht op verzet toegekend. Hiernaast heeft de betrokkene het recht om over de verwerking van zijn persoonsgegevens te worden geïnformeerd. Uitgangspunt is dat de diverse rechten de betrokkene in staat moeten stellen na te gaan welke

---

[57] Registratiekamer, 'Klant in het web. Privacywaarborgen voor Internettoegang', Den Haag, juni 2000, par. 6.4.2.

[58] *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 67.

[59] Zie onder meer de *Richtsnoeren Beveiliging van persoonsgegevens*, Cbp, Den Haag, februari 2013.

[60] 'Opinion 05/2012 on cloud computing', adopted July 1st 2012 by the Article 29 Data Protection Working Party (WP 196). Ook: Zienswijze inzake de toepassing van de Wet bescherming persoonsgegevens bij een overeenkomst met betrekking tot cloud computing diensten van een Amerikaanse leverancier, mededeling Cbp van 10 september 2012. Bron: http://www.cbpweb.nl/downloads_med/med_20120910-zienswijze-toepassing-wbp-SURFmarket-cloud-computing.pdf. Zie ook M.B. Voulon, 'Catch 22, Amerikaanse vorderingen tot het verstrekken van gegevens versus het verbod op doorgifte aan derde landen', *P&I* 2012/5, p. 214 e.v. enJ.M.A. Berkvens, Clou(d)(t)sourcing binnen de financiële sector, *FR* 2012/12.

[61] Zie hierover: Groep Gegevensbescherming artikel 29. Advies 3/2010 over het verantwoordingsbeginsel, 00062/10/NL WP 173.

[62] Zie bijvoorbeeld art. 10 van de Gedragscode verwerking persoonsgegevens financiële instellingen 2010.

hem betreffende gegevens met welke herkomst worden verwerkt en ze zonodig te laten corrigeren of verwijderen. Na de limitering van de genoemde rechten te hebben uiteengezet, bespreken we de rechten.

Limitering rechten

Van een aantal van de hiervoor behandelde rechten[63] kan geen gebruik worden gemaakt voor zover zwaarwegende belangen zich daartegen verzetten. Deze laatste belangen worden in art. 43 Wbp vermeld:

a. de veiligheid van de staat;
b. de voorkoming, opsporing en vervolging van strafbare feiten;[64]
c. gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
d. het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de veiligheid van de staat dan wel de voorkoming, opsporing en vervolging van strafbare feiten;
e. de bescherming van de betrokkene of de rechten en vrijheden van anderen.

Van belang is tevens te vermelden dat onder de term 'anderen' in onderdeel e ook de verantwoordelijke moet worden begrepen. Zo zal de verantwoordelijke indien hij voldoende aannemelijk weet te maken dat door inwilliging van een verzoek op kennisneming de administratieve lasten zodanig disproportioneel zijn dat hij in een van zijn rechten en vrijheden wordt aangetast, kennisneming kunnen weigeren.

Andere voorbeelden van toepasselijkheid van art. 43 sub e zijn onder meer de bescherming van auteursrechtelijke belangen[65] en de vrijheid van een ongestoorde gedachtewisseling.[66]

De tekst van art. 43 Wbp spreekt over toepassing 'voor zover noodzakelijk'. Dit betekent dat er sprake dient te zijn van een absolute noodzaak. Indien de noodzaak slechts bestaat ten aanzien van een deel van de gegevens gelden de diverse rechten wel onverkort ten aanzien van de andere gegevens. De term 'voor zover' kan ook slaan op een beperking in de tijd die een tijdelijk karakter heeft. Het doorvoeren van een correctie kan bijvoorbeeld mogelijk worden uitgesteld totdat een geplande grote onderhoudsbeurt aan een computersysteem plaatsvindt. In de Dexia-zaken is bepaald dat bij het uitoefenen van het recht op inzage niet te snel mag worden aangenomen dat sprake is van misbuik van recht in de zin van art. 3:13 BW.[67] Het inzagerecht wordt beschouwd als een zelfstandig recht naast de art. 843a en b van het Wetboek van burgerlijke rechtsvordering.

Art. 44 Wbp maakt een uitzondering op de informatieplicht van art. 34 Wbp en het recht op inzage (art. 35 Wbp) indien de verwerking van persoonsgegevens plaatsvindt door instellingen en diensten voor wetenschappelijk onderzoek of statistiek. Wel dient de verantwoordelijke er zorg voor te dragen dat de nodige voorzieningen zijn getroffen om te verzekeren dat de persoonsgegevens uitsluitend voor statistische en wetenschappelijke doeleinden worden gebruikt. De ratio achter de uitzondering is gelegen in de onevenredige inspanning die het informeren van de betrokkene dan wel het voldoen aan een inzageverzoek met zich mee zou brengen. De term 'nodige' duidt dan ook op een proportionaliteit tussen het belang van de bescherming van persoonsgegevens enerzijds en de kosten en inspanningen die zijn verbonden aan de effectuering van de genoemde rechten anderzijds. De aard van de proportionele maatregel zal daarbij wijzigen met de ontwikkeling van de stand van de techniek.

In een uitzondering op de informatieplicht is tevens voorzien wanneer de verwerking betreft van persoonsgegevens die deel uitmaken van archiefbescheiden die ingevolge de Archiefwet zijn overgebracht naar een archiefbewaarplaats (art. 44 lid 2 Wbp). Ook hier is de ratio achter deze uitzondering gelegen in de onoverkomelijke problemen die – gezien de grote hoeveelheden archiefbescheiden – het informeren van betrokkenen met zich mee zou brengen.

Ten slotte zij opgemerkt dat met een beroep op artikel 43 de verenigbaarheidstoets van art. 9 Wbp terzijde kan worden gesteld. Dat gebeurt bijvoorbeeld als een bedrijf overweegt in het kader van een strafrechtelijk onderzoek op basis van art. 8, onder *f*, Wbp gegevens ter beschikking van de politie te stellen.

Kennisgeving

De Wbp kent een aantal verplichtingen om de betrokkene te informeren omtrent diverse aspecten van de informatieverwerking. De wet onderscheidt twee situaties van gegevensverwerking waarin de betrokkene op de

---

[63] Het betreft de algemene informatieplicht jegens eenieder (art. 30 lid 3, Wbp), de informatieplicht tegenover de betrokkene (art. 33 en 34 Wbp) en het recht op kennisneming en correctie (art. 35 Wbp). De uitzonderingen zien tevens op het beginsel van verenigbaar gebruik (art. 9 Wbp.

[64] Onderdeel b. kan vermoedelijk ook door verantwoordelijken buiten het justitiële apparaat worden ingeroepen. Dit volgt uit art. 22 Wbp. Anders M.M. Koevoets, *Wangedrag van werknemers - De bevoegdheid van werkgevers tot opsporing en sanctionering*, Boom 2006, p. 35.

[65] Zie P&I 2008/5 nrs. 250 en 263.

[66] Rb. 's-Gravenhage, 27 december 2005, nr. AWB *0515365* WPD. Gepubliceerd in Uitsprakenbundel Wet bescherming persoonsgegevens, van Dijk e.a. (red.), Den Haag, SDU 2009. Zie nr. 43.2.

[67] HR 29 juni 2007,*LJN* AZ4663 en HR 29 juni 2007 *LJN* AZ4664.

hoogte moet worden gebracht: 1) wanneer de persoonsgegevens worden verkregen bij de betrokkene zelf en 2) wanneer de gegevens op een andere wijze worden verkregen.[68]

Op de eerste plaats geldt de verplichting van art. 33 Wbp om bij het verzamelen van gegevens bij de betrokkene zelf deze *voorafgaand*[69] aan het moment van verkrijging nader te informeren over onder meer de identiteit van de voor de verwerking verantwoordelijke, de doeleinden van de gegevensverwerking, de ontvangers en een eventuele overdracht naar derde landen.[70] In de praktijk zal deze plicht veelal vorm krijgen door de betreffende informatie te vermelden op een bij verkrijging te overhandigen standaardformulier. Mededeling is niet nodig indien de betrokkene op de hoogte is van de verkrijging van de gegevens door het bedrijf of de organisatie die de gegevens verwerkt. De formulering dat de betrokkene op de hoogte moet zijn, is stringenter dan de "redelijkerwijze op de hoogte is". Voor wat betreft het tijdstip van mededeling is de formulering van dit artikel eveneens stringenter dan die in het hierna te bespreken art. 34 Wbp. De ratio is dat de wetgever ervan uitgaat dat bij het van de betrokkene verkrijgen van gegevens ook inderdaad de mogelijkheid bestaat hem de opgesomde informatie vooraf te verstrekken. Een praktisch probleem kan zich mogelijk voordoen indien sprake is van het maken van beeld- of geluidopnames.

Wanneer de gegevens op aan andere wijze worden verkregen gelden de bepalingen van art. 34 Wbp. Als voorbeeld noemen we het verkrijgen door een internet-provider van persoonsgegevens naar aanleiding van het beheer van een netwerk. 'Voorzover een provider kan worden aangemerkt als een beheerder van een netwerk houdt dit in dat hij gegevens verkrijgt door eigen observatie bij het vastleggen van de clickstreams van de individuele abonnee. Er is dus geen sprake van gegevensverkrijging van de betrokkene maar van een verkrijging op andere wijze.'[71] In de gevallen van verkrijging uit andere bron dient de informatie aan de betrokkene te worden verstrekt op het moment van vastlegging dan wel uiterlijk op het moment van de eerste verstrekking aan een derde indien de gegevensverwerking daartoe bestemd is. Ook hier is mededeling niet nodig indien de betrokkene op de hoogte is van de verkrijging van de gegevens door het bedrijf of de organisatie die de gegevens verwerkt. Tevens gelden in deze situatie aanvullende uitzonderingen: het informeren van de betrokkene blijkt onmogelijk, de mededeling kost een onevenredige inspanning of de verstrekking bij of krachtens de wet is voorgeschreven[72]. Deze laatste situatie vormt de uitzonderingsgrond voor vele verwerkingen door de overheid en betekent – ons inziens overigens geheel in strijd met de ratio achter privacybescherming en meer specifiek een van de belangrijke doelstellingen van de nieuwe wet (namelijk transparantie) – dat betrokkenen in vele gevallen niet zullen worden geïnformeerd over gegevensverwerkende processen bij de overheid.[73]

Ten slotte legt art. 41 lid 3 Wbp de verantwoordelijke die gegevens verwerkt ten behoeve van direct marketing doeleinden (charitatief dan wel commercieel) een informatieplicht op ten aanzien van de mogelijkheid tot het doen van verzet tegen deze verwerking. Art. 41 vormt vanuit wetsystematisch oogpunt een fremdkörper in de Wbp. Het betreft namelijk een regeling die uitdrukkelijk ingaat op de inhoud en de vorm van communicatie en daarmee een onderwerp op het gebied van de relationele privacy aansnijdt. Artikel 41 is in 2012 gewijzigd.[74]

In diverse bepalingen in de Telecommunicatiewet worden aan de verantwoordelijke eveneens informatieplichten opgelegd.[75] Het gaat daarbij om het informeren over mogelijk gebruik van telefoonnummers en mailadressen voor commerciële doeleinden, het gebruik van cookies en van locatiegegevens.

In voorbereiding is een aanpassing van de Wbp waarbij datalekken moeten worden gemeld bij het Cbp en bij de betrokkene.[76]

Ten slotte wordt een voorstel voorbereid tot melding van cyber-incidenten, dat een algemene strekking heeft maar deels overlapt met de meldplicht bij datalekken.[77]

---

[68] E. Verhelst, *Recht doen aan privacyverklaringen* (diss: Tilburg UVT), Tilburg: 2012.

[69] De formulering is wellicht ook restrictiever dan die van de Europese Richtlijn die de term 'voorafgaand' niet hanteert.

[70] Naar aanleiding van de zogenaamde Swift-case publiceerden de Nederlandse banken een mededeling in de kranten dat bij de afhandeling van het betalingsverkeer gegevens buiten Europa terecht konden komen en daardoor ook onder rechtsmacht van buitenlandse opsporingsinstanties konden vallen. Deze tekst maakt nu onderdeel uit van de per 1 november 2009 ingevoerde nieuwe algemene bankvoorwaarden.

[71] Registratiekamer, 'Klant in het web', Den Haag, juni 2000, par. 6.6.1.

[72] *Klant te koop, Privacyregels voor adressenhandel*, CBP AV24; van Eijk; van Helden: "Het CBP acht het verdedigbaar dat het vasthouden aan het in artikel 34 bepaalde *moment* van informeren onevenredige inspanning kost en dat een geslaagd beroep op de uitzondering kan worden gedaan. Dit ontslaat de ontvanger van de adressen niet van de informatieplicht, maar geeft hem de ruimte om deze te combineren met de werkelijke Dmmailing." (zie p.34 van de achtergrondstudie).

[73] Zie nader over het belang van transparantie bij gegevensverwerking door de overheid: J.E.J. Prins, "Technocratie en de toekomstagenda van de Nationale Ombudsman", in: Werken aan behoorlijkheid. De Nationale Ombudsman in zijn context (jubileumbundel 25 jaar Nationale Ombudsman), Den Haag: Boom Juridische Uitgevers 2007, pp. 111-134.

[74] Zie *Stb*. 2012, 33.

[75] Zie *Stb* 2012, 235.

[76] Art. 34a van het consultatiedocument van december 2011: Wijziging Wbp (gebruik camerabeelden en meldplicht datalekken), consultatiedocument ministerie van V&J 20/12/2011. *Kamerstukken II*, 2012/13, 33 662, Wijziging van de Wet bescherming persoonsgegevens en de Telecommunicatiewet in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (gebruik meldplicht datalekken).

Kennisneming ("recht op inzage")

In aanvulling op de voornoemde actieve informatieplichten van de verantwoordelijke, kan men bij een verantwoordelijke informeren of hem of haar betreffende gegevens worden verwerkt.[78] De verwerker zal de benodigde informatie dan dienen te verstrekken, waarbij hij zich overigens dient te vergewissen van de identiteit van de betrokkene (art. 37 Wbp).[79] Op de eerste plaats is dat de situatie van art. 30 lid 3 Wbp. Wanneer het een van aanmelding vrijgestelde verwerking betreft is de verantwoordelijke verplicht *een ieder* die daarom verzoekt de inlichtingen te verschaffen die anders bij de aanmelding zouden zijn verstrekt.[80] Het betreft hier dus een algemene informatieplicht. Het resultaat van deze verplichting is dat het principe van de genormeerde vrijstelling op dit punt niet veel betekenis heeft omdat de verantwoordelijke de betreffende informatie toch zal moeten bijhouden.

Op de tweede plaats kunnen betrokkenen zich tot de verantwoordelijke richten met het verzoek of hem betreffende gegevens worden verwerkt (art. 35 Wbp). Inmiddels is er een aanzienlijke hoeveelheid jurisprudentie en litteratuur over dit onderwerp verschenen.[81] De verantwoordelijke moet binnen vier weken antwoorden. Naast de informatie betreffende de herkomst van de gegevens, de categorieën van gegevens, de doeleinden van verwerking en de ontvangers, zal de verantwoordelijke desgevraagd een mededeling moeten doen omtrent de logica die ten grondslag ligt aan de geautomatiseerde verwerking van hem betreffende gegevens.

Alvorens de betreffende informatie aan de betrokkene ter beschikking te stellen, is de verantwoordelijke gehouden een derde, op wie de informatie eveneens betrekking heeft, en die tegen het ter beschikking stellen van deze informatie naar verwachting bedenkingen heeft in de gelegenheid te stellen zijn zienswijze naar voren te brengen. Te denken valt hier bijvoorbeeld aan de situatie dat een ex-echtgenoot inzage wenst in een dossier bij de sociale dienst, waarin persoonsgegevens over de ex-partner zijn opgenomen.

In de Engelse rechtszaak Durant versus FSA is door de hogere rechter bepaald dat het enkele voorkomen van iemands naam in een registratie onvoldoende is om hem recht op inzage te geven. Het gebruik van privacyregels om een procesdossier op te bouwen is volgens die rechter een vorm van misbruik van recht.[82] In de Dexiazaken oordeelde de Hoge Raad tegenovergesteld.[83]

Bij het geven van inzage is ook de vorm waarin inzage wordt gegeven van belang. In beginsel strekt het inzagerecht zich uit tot een overzicht van de verwerkte gegevens. Volgens de Hoge Raad kan het soms nodig zijn om een (al dan niet deels afgeschermde) kopie van het document waarin de verwerkte gegevens zijn opgenomen aan de verzoeker te verschaffen.[84] De Raad van State lijkt daarentegen een strakker onderscheid te maken tussen gegevensdrager en persoonsgegevens.[85] Inmiddels hebben zowel de Rechtbank Middelburg[86] als de Raad van State[87] prejudiciele vragen aan het Europese Hof van Justitie gesteld over de interpretatie van het inzagerecht.

---

[77] Concept 16 juli 2013 t.b.v. consultatie Wet houdende regels over het melden van een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving (Wet melding inbreuken elektronische informatiesystemen).

[78] Het moet gaan om nog aanwezige informatie. Er is geen sprake van een reconstructieplicht. Zie Uitsprakenbundel Wet bescherming persoonsgegevens, van Dijk e.a. (red.), Den Haag, SDU 2009. Zie nr. 35.8.

[79] Uitsprakenbundel Wet bescherming persoonsgegevens, van Dijk e.a. (red.), Den Haag, SDU 2009. Zie nr. 37.1. Zie ook Rechtbank Arnhem, zaaknummer/rekestnummer 171494 /HA RK 08-177 d.d. 6 oktober 2008.

[80] De betreffende inlichtingen worden genoemd in art. 28 lid 1, onder *a-e* Wbp.

[81] W.A.K. Rank en A.J. Haasjes, Misbruik van de Wbp in civiele procedures tegen financiële instellingen, *Tijdschrift voor financieel recht* 2005/12; G.J. Zwenne & J. Webbink 'De winstverdubbelaar en de Wbp: over de reikwijdte en inhoud van het kennisnemingsrecht van artikel 35', *P&I* 2006, 2, p.1-8; G-J. Zwenne, Nogmaals de WBP en de winstverdubbelaar, *Computerrecht* 2007/172; J.P. van Schoonhoven, 'Inzage bij banken; een recht te ver?', *Computerrecht* 2006, 99; J.M.A. Berkvens, 'Inzage, inzicht of overzicht', *P&I* 2005, p. 119-121; A.J.E. van den Bergen, 'De Wet bescherming persoonsgegevens in de financiële procespraktijk', *Tijdschrift voor Financieel Recht*, 2005, 10, p. 296-306; A.D. Putker-Blees en A. Meulenveld, Inzicht in het inzagerecht, *Tijdschrift Recht en Arbeid*, nr. 2006/10; P.J.A. de Hert e.a., *'De WBP na de Dexia·uitspraken', P&I* 2007-4, p. 147-157; J. Holvast. 'Annotatie bij Rb. Amsterdam 19 mei 2005', *Computerrecht* 2005, 49. p. 323-327; G·J. Zwenne e.a., *Eerste fase evaluatie Wet bescherming persoonsgegevens, Litteratuuronderzoek en knelpuntenanalyse*, WODC 2007; J.M.A. Berkvens, Wob-verzoek om inzage in politieregister, noot bij ABRvS, s-Gravenhage 29 november 2006, nr. 200601984/1, LJN AZ3237, Privacy &Informatie 2007/1, p. 25/26; C.M. Jakimowic, J.M.A. Berkvens, "De spelregels bij verzoeken tot inzage op grond van de Wbp", *Privacy en Informatie* 2013, nr. 2; M. Jansen, "Over het inzagerecht en het bestandsbegrip", *Privacy en Informatie* 2013, nr. 2.

[82] [2003] EWCA Civ 1746 Case No: B2/2002/2636 8th December 2003, Zie overwegingen 27, 30 en 31.

[83] Onder meer LJN: AZ4663, Hoge Raad , R06/045HR d.d. 29-06-2007 (Dexia-1); R.O. 3.6.1.

[84] LJN: AZ4663, Hoge Raad , R06/045HR d.d. 29-06-2007 (Dexia-1); R.O. 3.4.
LJN: AZ4664, Hoge Raad , R06/046HR d.d. 29-06-2007 (Dexia-2); R.O. 3.4.

[85] Afdeling bestuursrechtspraak, Raad van State nr. 200601984/1, LJN AZ3237 d.d. 29 november 2006 (onderscheid gegevens en gegevensdrager). Zie ook Uitsprakenbundel Wet bescherming persoonsgegevens, van Dijk e.a. (red.), Den Haag, SDU 2009. Zie nr. 35.6. Zie RO 2.5.1.

[86] Rb. Middelburg, 15 maart 2012, LJN BV8942.

[87] ABRvS,3 augustus 2012, Zaak C-372/12.

Op grond van art. 39 Wbp mag de verantwoordelijke kosten in rekening brengen. Daarbij mag tot op zekere hoogte ook rekening worden gehouden met de werkelijk door de verantwoordelijke te maken onkosten.[88]

Correctie

Art. 36 Wbp bepaalt dat degene aan wie kennis is gegeven van hem betreffende persoonsgegevens, de verantwoordelijke kan verzoeken deze gegevens te verbeteren, aan te vullen, te verwijderen, of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet terzake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het correctierecht expliciteert met deze formulering de mogelijkheid om gegevens die niet mogen worden verwerkt af te schermen in plaats van ze te verwijderen. De Wbp kent in art. 38 een verplichting tot kennisgeving aan derden van alle gerectificeerde, uitgewiste of afgeschermde gegevens. Er is geen sprake van een protocolplicht. Daar staat tegenover dat de verwerker een zekere inspanning zal moeten plegen om te reconstrueren aan wie hij eerder gegevens heeft verstrekt. Alleen wanneer kennisgeving aan derden onmogelijk blijkt dan wel een onevenredige inspanning kost, zal deze achterwege kunnen blijven. De bepaling heeft een terugwerkende kracht die in beginsel niet beperkt is in de tijd.

Verzet

Onder de Wbp wordt aan degene van wie persoonsgegevens worden verwerkt een recht op verzet toegekend (art. 40 en 41 Wbp). De betrokkene heeft dit recht op verzet wanneer zijn gegevens worden verwerkt voor de goede vervulling van een publiekrechtelijke taak (art. 8 onder *e* Wbp) dan wel voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of een derde aan wie de gegevens worden verstrekt (art. 8, onder *f*, Wbp). In deze gevallen zal een afweging dienen plaats te vinden tussen de bijzondere omstandigheden van de betrokkene enerzijds en de belangen van de verantwoordelijke anderzijds. Met andere woorden, betrokkenen kunnen slechts een beroep op het recht van verzet doen indien zij een gerechtvaardigd individueel belang kunnen aantonen.

Het recht op verzet geldt onvoorwaardelijk de verwerking van persoonsgegevens ten behoeve van direct marketing doeleinden (charitatief dan wel commercieel). In de praktijk betekent dit dat dergelijke bedrijven en instellingen een afzonderlijk gegevensbestand zullen moeten aanhouden met de namen van de personen die van hun recht op verzet gebruikmaken.

Daarnaast is op grond van art. 11 lid 7 van de telecommunicatiewet het zogenaamde "Belmenietregister" in het leven geroepen.[89] Artikel 11 lid 7 van de telecommunicatiewet kent overigens een uitgebreide regeling voor het recht van verzet tegen benadering via de openbare telecommunicatie-infrastructuur. Ook kan worden verwezen naar art. 7:46h BW en art. 81 van het Besluit Gedragstoezicht financiële ondernemingen. Artikel 11 lid 5a van de telecommunicatiewet legt het commerciële gebruik van locatiegegevens aan banden.

Geautomatiseerde beslissingen

In de Wbp is in art. 42 een regeling opgenomen die betrekking heeft op het langs geautomatiseerde weg nemen van beslissingen op basis van persoonlijkheidsprofielen. Het betreft een uit de Franse privacywetgeving afkomstige bepaling. Het eerste lid kent aan eenieder het recht toe, behoudens onder de in het tweede lid genoemde omstandigheden en waarborgen, niet te worden onderworpen aan een besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem in aanmerkelijke mate treft, indien dat besluit alleen wordt genomen op grond van een geautomatiseerde gegevensverwerking betreffende bepaalde aspecten van iemands persoonlijkheid (beroepsprestatie, kredietwaardigheid, gedrag, en dergelijke).[90] Zo zal in situaties waarin de beslissing tot het verlenen van een krediet geautomatiseerd wordt afgehandeld, toch een menselijke afweging in het systeem dienen te worden geïmplementeerd.

In het tweede lid van art. 42 Wbp wordt bepaald dat een geautomatiseerd besluit desalniettemin kan worden genomen indien dit besluit wordt genomen in het kader van het sluiten of uitvoeren van een overeenkomst en aan het verzoek van de betrokkene is voldaan dan wel passende maatregelen (dat wil zeggen de betrokkene is in de gelegenheid gesteld omtrent het besluit zijn zienswijze naar voren te brengen) zijn genomen ter bescherming van zijn gerechtvaardigde belang. Het besluit kan eveneens op geautomatiseerde wijze worden genomen indien het zijn grondslag vindt in een wet waarin maatregelen zijn vastgesteld die strekken tot bescherming van dit

[88] Uitsprakenbundel Wet bescherming persoonsgegevens, van Dijk e.a. (red.), Den Haag, SDU 2009. Zie nr. 39.1. Ook Rechtbank Arnhem, zaaknummer/rekestnummer 171494 /HA RK 08-177 d.d. 6 oktober 2008. Bevestigd door het Hof Arnhem in haar beschikking met zaaknr. 200.021.810 d.d. 1 sept. 2009.
[89] Besluit van 26 februari 2009, Stb 2009, 129.
[90] Zie: M.M. Groothuis, "Geautomatiseerde besluitvorming voor beschikkingen: aspecten van privacyrecht", hoofdstuk 3, pp. 55-74.

gerechtvaardigde belang. Indien de in lid 2 genoemde uitzonderende omstandigheden en waarborgen van toepassing zijn dient de betrokkene in ieder geval op de hoogte gesteld te worden van de logica die ten grondslag ligt aan de geautomatiseerde verwerking.

Zelfregulering

De Wbp geeft ruimte voor zelfregulering. Naast gedragscodes op nationaal niveau wordt ook voorzien in de mogelijkheid van internationale gedragscodes. De Wbp kent de mogelijkheid van een gedragscode vervangende algemene maatregel van bestuur voor het geval de zelfregulering in een bepaalde sector onvoldoende van de grond zou komen. Het Cbp toetst of is voldaan aan het vereiste *dat de regels een juiste uitwerking moeten vormen van de wet.*

Inmiddels zijn diverse nationale gedragscodes tot stand gekomen. Chronologisch zijn dat onder meer de gedragscodes van Nefarma, financiële sector, handelsinformatiebureaus, particuliere recherche, gerechtsdeurwaarders en onderzoek & statistiek. Enkele gedragscodes zijn inmiddels verlopen en alweer vervangen door vernieuwde versies. Als voorbeeld van een internationale gedragscode kan de Fedma-code voor de marketing industrie worden genoemd .[91] Deze gedragscode wordt door de DDMA aan haar leden voorgeschreven.

Handhaving[92]

De Wbp kent een drietal handhavingssystemen. Op der eerste plaats een civielrechtelijk systeem waarbinnen de betrokkene onder meer de mogelijkheid heeft van laagdrempelige toegang tot de gewone rechter[93] en het recht op vergoeding van immateriële schade.[94] Op de tweede plaats is er een administratiefrechtelijk systeem waarbinnen het Cbp onder meer toezichthoudende en interventiebevoegdheden bezit inclusief de mogelijkheid een bestuurlijke boete op te leggen[95].Het Cbp heeft in dat verband ook de mogelijkheid om ambtshalve of op verzoek van een betrokkene een onderzoek in te stellen. Tenslotte werkt de Wbp met een strafrechtelijk systeem waarin onder meer het niet aanmelden van een persoonsregistratie als een strafbaar feit wordt gedefinieerd.

Het administratiefrechtelijke handhavingsysteem heeft gedurende de parlementaire behandeling van de Wbp diverse veranderingen ondergaan. Zo was de mogelijkheid om bestuurlijke boetes op te leggen in eerste instantie geschrapt om later weer terug te keren. De invoering van nieuwe tranches van de Awb heeft ook invloed gehad op het administratiefrechtelijke handhavingssyteem. Ten slotte zij vermeld dat er een mogelijkheid is gekomen om klachten over het Cbp neer te leggen bij de Nationale Ombudsman. Het Cbp heeft er voor gekozen om haar rol van adviseur af te bouwen en haar rol van handhaver verder te versterken. In het kabinetsstandpunt inzake de evaluaties van de Wbp worden voorstellen aangekondigd om deze lijn verder uit te werken.[96]

In het kader van het handhavingsysteem besteden we nog aandacht aan een tweetal speciale figuren in de Wbp. In de Wbp wordt naar Duits model de functionaris voor de gegevensbescherming geïntroduceerd. Deze kan worden aangesteld op het niveau van een rechtspersoon of op het niveau van een koepelorganisatie. Op grond van art. 64 Wbp ziet de functionaris toe op de verwerking van persoonsgegevens door de verantwoordelijke die hem heeft benoemd (of door de leden van de koepel die hem heeft aangesteld).[97] De betreffende organisatie dient de aanstelling van de functionaris te melden bij het College Bescherming Persoonsgegevens. Een verantwoordelijke die onder het toezicht van een dergelijke functionaris valt geniet vrijstelling van de aanmeldingsplicht voor verwerkingen.[98] De wet stelt als voorwaarde dat de functionaris over voldoende kennis beschikt en betrouwbaar is (wat dat laatste vereiste inhoudt moet overigens worden afgewacht). Verder geldt als voorwaarde dat de betreffende persoon zijn taken in relatieve onafhankelijkheid dient te kunnen verrichten. Tenslotte is van belang er op te wijzen

---

[91] Goedgekeurd door de artikel 29 werkgroep op 13 juni 2003 (Opinion 3/2003).

[92]Voor een gedetailleerd commentaar verwijzen we naar J.H.J. Terstegge*, 'Van de regen en de drup'*, Nederlands Tijdschrift voor Bestuursrecht, 2000, p.243-251 en naar het hoofdstuk *'Privacyregulering en de AWB'* van A.E. Schilder in: J.E.J. Prins & J.M.A. Berkvens (red.), Privacyregulering in theorie en praktijk, 2e druk, Deventer 2000, p.117-134.

[93] Artt. 45 en 46 Wbp.

[94] Art. 49 Wbp. Zie: A. Mitrakas, "Assessing Liability arising from information security breaches in data privacy", *International Data Privacy Law*, March 2011; K. de Vulder, B. Bruyndonckx, "Aansprakelijkheidsclausules in de cloud", Afl. 3 juni 2011, *Computerrecht*, pp.123-128.

[95] Zie de boeteregeling in Stcrt. 2003, nr. 123 p. 27.

[96] *Kamerstukken II*, 2009/10, 31051, nr. 5.

[97] De functionaris geniet ontslagbescherming op grond van art. 7:670a BW.

[98]Waarbij overigens geldt dat een organisatie ook een privacyfunctionaris kan aanstellen zonder deze te melden bij het College Bescherming Persoonsgegevens. Het gevolg is dan wel dat in dat geval de vrijstelling van de meldingsplicht niet geldt. Het is aan iedere individuele organisatie om de afweging te maken of het instellen van een officiële privacyfunctionaris wenselijk is.

dat de privacyfunctionaris geen rapportageplicht aan het College Bescherming Persoonsgegevens heeft. Ook in dit opzicht dient de functionaris redelijk autonoom te functioneren.

De tweede figuur is die van het voorafgaand onderzoek. De Europese Richtlijn voorziet in de – facultatieve – optie van de figuur van voorafgaand onderzoek. De nationale wetgever heeft deze mogelijkheid aangegrepen door een aantal verwerkingen aan voorafgaand toezicht van het Cbp te onderwerpen. Ratio achter de regeling is dat aan dergelijke verwerkingen een bijzonder risico is verbonden. Het betreft momenteel verwerkingen waarbij een persoonsnummer wordt gebruikt, verwerkingen waarbij strafrechtelijke gegevens worden gebruikt zonder dat daarvoor een wettelijke basis is en verwerkingen waarbij de gegevens zijn verzameld zonder het medeweten van de betrokkene. Het aantal onder dit regime vallende verwerkingen is op een later tijdstip bij AMvB uit te breiden, waarbij het – niet nader omschreven – risicokarakter van de verwerking aanknopingspunt is. Blijkens art. 32 Wbp kan het voorafgaand onderzoek een tijdsbeslag van 24 weken vragen. De procedure bestaat uit 2 fasen. Na de melding onderzoekt het Cbp of een nader onderzoek noodzakelijk is. Voor de eerste fase staat een periode van maximaal 4 weken. Het nadere onderzoek duurt maximaal 20 weken. De regeling van het voorafgaand onderzoek is in 2012 gewijzigd.[99] Bij veel voorkomende typen van verwerkingen hoeft niet steeds een voorafgaand onderzoek te worden aangevraagd als er al eerder een vergelijkbaar onderzoek heeft plaats gehad.

Meldingssysteem

De Wbp kent een aanmeldingssysteem. Dit systeem is voor overheid en particuliere sector gelijkgeschakeld. Het aanmeldingsformulier moet zowel het verzameldoel bevatten als een omschrijving van de uiteindelijke verwerkingsdoeleinden. Indien op enig moment verwerkingen plaatsvinden die niet in overeenstemming zijn met de oorspronkelijke aanmelding dient dat op grond van art. 28 lid 4 gedurende drie jaar te worden geprotocolleerd. Aanmelding vindt plaats bij het College tenzij de verantwoordelijke een *functionaris voor de gegevensverwerking* heeft aangesteld. In dat geval kan vanwege art. 27 aanmelding bij de functionaris plaatsvinden. Ten aanzien van veel voorkomende transparante verwerkingen kan bij AMVB worden bepaald dat aanmelding achterwege kan blijven. Het vrijstellingsbesluit is in 2012 uitgebreid met een aantal nieuwe vrijstellingen.[100] Aanmelding kan zowel via een schriftelijk aanmeldingsformulier, als op elektronische wijze.[101] In 2012 is een aanpassing van de Wbp in werking getreden waarbij op niet aanmelden van een verwerking zwaardere straffen worden gezet.[102]

De internationale dimensie[103]

Algemeen

Met name ten gevolge van de introductie van ICT-toepassingen als elektronisch betalingsverkeer, internet, social media en allerlei vormen van elektronische handel heeft het internationale persoonsgegevensverkeer een enorme vlucht genomen. In relatie tot de Wbp spelen twee aspecten een rol. Allereerst de vraag in hoeverre en onder welke voorwaarden persoonsgegevens naar het buitenland mogen worden geëxporteerd. Daarnaast de vraag onder welke omstandigheden de Wbp van toepassing is.[104]

Export naar derde landen

Vanuit het perspectief van een Europese interne markt, zien de voorschriften inzake de export van persoonsgegevens uitsluitend op een doorvoer naar landen buiten de Europese Unie (derde landen). De betreffende bepalingen zijn neergelegd in art. 76-78 Wbp. Als uitgangspunt voor de doorgifte naar een derde land geldt dat die uitsluitend mag plaatsvinden naar landen waarvan de wet- en regelgeving een passend beschermingsniveau biedt. Voor het oordeel of een bepaald beschermingsniveau al dan niet als *passend* kan worden gekwalificeerd, wordt in het tweede lid van art. 76 Wbp een aantal voor de doorgifte relevante omstandigheden genoemd.[105]

---

[99] *Zie: Stb.* 2012, 33.
[100] Zie: Stb. 2012, 90.
[101] Zie: *Stb.* 2001, 337.
[102] Zie: Stb. 2012, nr. 33.
[103] *Kamerstukken II 27 043, nr. 1, Toepassing van art. 25 en 26 van Richtlijn 95/46/EG (gegevensverkeer tussen de EU en derde landen).*
[104] Zie over de grote diversiteit aan regels op een mondiaal niveau en meer in het bijzonder de regels betreffende de export van persoonsgegevens in een groot aantal landen van de wereld: Kuner, C. *Transborder Data Flow Regulation in Data Protection and Privacy Law*, diss. Universiteit Tilburg 2012.
[105] Genoemd worden: de aard van de gegevens. Zo zal het feit dat het bij de doorgifte om gevoelige gegevens gaat tot een andere kwalificatie inzake

Het zal niet verbazen dat de Europese ontwikkelingen inzake de doorgifte naar derde landen in de Verenigde Staten met argusogen worden gevolgd. De Verenigde Staten en de Europese Unie hebben er lang over gedaan om tot overeenstemming te komen over de wijze waarop het eerstgenoemde land aan de voorwaarden van de Privacyrichtlijn zal voldoen.[106] Centraal staan hierbij de zogenaamde 'International Safe Harbour Principles'.[107] Deze Principles beogen een bepaalde mate van rechtszekerheid te bieden aan Europese verwerkers van persoonsgegevens dat ze handelen in overeenstemming met de bepalingen van de Europese Richtlijn wanneer zij persoonsgegevens verstrekken aan organisaties die op vrijwillige basis deze Principles onderschrijven. In de Verenigde Staten zullen de Federal Trade Commission en het Ministerie van Vervoer toezien op de handhaving van de Principles.[108]

Over de Safe Harbour Principles verscheen in juli 1999 een discussiestuk van de artikel 29-Groep[109], welk document een belangrijke rol speelde bij de onderhandelingen tussen de Verenigde Staten en de Europese Unie. Mede naar aanleiding van dit discussiestuk verscheen in november 1999 een nieuwe versie van de Principles.[110] Op 15 maart 2000 werd na maanden van moeizame onderhandelingen over de inhoud en de handhaving van de Principles een principeakkoord bereikt tussen vertegenwoordigers van de Verenigde Staten en de Europese Unie. Uiteindelijk kon het akkoord, ondanks tegenstand van het Europees Parlement, in de zomer van 2000 worden geformaliseerd.[111] Daarmee heeft de Europese Commissie de aanpak van privacybescherming via zelfregulering met als stok achter de deur handhaving door overheidsinstanties als een manier erkend waarmee aan de voorwaarde van adequate bescherming kan worden voldaan.[112]Zoals al eerder in dit hoofdstuk is besproken, woedt de transatlantische discussie echter onverminderd voort. Die heeft met name betrekking op de uitwisseling van allerhande gegevens in het kader van de terrorisme bestrijding.[113] Een ander voorbeeld wordt gevormd door Amerikaanse fiscale wetgeving op basis waarvan wereld wijd financiële instellingen verplicht worden om te rapporteren over inkosten van US-citizens (FATCA).[114] Een deel van de angel wordt inmiddels uit de discussie gehaald door het afsluiten van bilaterale verdragen tussen de Verenigde Staten en afzonderlijke Europese landen. De Nederlandse tekst is nog niet gepubliceerd ten tijde van het afsluiten van dit hoofdstuk.[115] Nieuwe discussies zijn ontstaan naar aanleiding van het afluisterschandaal waarbij inlichtingendiensten op grote schaal het internetverkeer afluisteren (o.a. Prism surveillance programma van de US National Security Agency).

'passend' kunnen leiden dan waar het niet-gevoelige gegevens betreft; de doeleinden en de duur van de verwerking. Zo zal het bijvoorbeeld relevant kunnen zijn of persoonsgegevens eenmalig voor een boeking op een internationale vlucht worden uitgewisseld of voor langdurig gebruik ten behoeve van fraudebestrijding; het land van herkomst en het land van eindbestemming. Te denken valt hier aan de privacyreputatie van het betreffende land, de algemene en sectoriële rechtsregels die in het betrokken derde land gelden. Naast een algemene wet die de bescherming van persoonsgegevens regelt kan hier bijvoorbeeld worden gedacht aan specifieke regels zoals bijvoorbeeld voor de medische sector; de in het derde land nageleefde beroepscodes. Hier kan worden gedacht aan codes zoals die bijvoorbeeld in de direct marketing branche worden gehanteerd; de veiligheidsmaatregelen die in het derde land worden gehanteerd. Zijn er bijvoorbeeld specifieke regels gesteld ten aanzien van de beveiliging van de voor de gegevensverwerking gebruikte systemen?

[106]Zie ook: C.J. Bennit & Ch.D. Raab, 'The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response', *The Information Society* 13: 245-263.

[107]Zie: H. Rowe, EU Data Protection. 'The International Safe Harbour Principles', *Computer Law & Security Report* 2000, p. 41-42.

[108]Voor een uitvoerig artikel zij verwezen naar Wisman, 'Internationale gegevensuitwisseling. De Wbp in de praktijk', *Privacy en Informatie* 2001, p. 9. Intussen leert de website van het US Department of Commerce dat de animo onder het Amerikaanse bedrijfsleven niet erg groot is (www.export.gov/safeharbor).

[109]Reference nr. 5075/99/EN/final. Zie ook: 'How to assess adequate protection: suggestions for ways forward', *Privacy Laws & Business International Newsletter* 1999, p. 4-6.

[110]Zie ook: Diana Alonso Blas, 'Towards a uniform application of the European Data Protection Rules, The role of the Article 29 Working Party', *Privacy & Informatie* 2001, p. 4-8.

[111] Zie Bloem, *Safe Harbour en het Amerikaanse beschermingsniveau*, Privacy & Informatie 2004/2 over praktische gevolgen van safe harbour.

[112]Voor meer informatie, zie: http://europa.eu.int/comm/internal_market/en/index.htm. De beslissing d.d. 26/7/2000 van de Europese Commissie is gepubliceerd in *PbEG* 2000 L 215/7.

[113] Hoboken, J.V.J. van en A.M. Arnbak , N.A.N.M. van Eijk, m.m.v. N. Kruijssen, ' Cloud diensten in hoger onderwijs en onderzoek en de USA Patriot Act', *Instituut voor Informatierecht* (UVA), Amsterdam: september 2012.

[114] Foreign Account Tax Compliance Act.

[115] De UK information commissioner publiceerde een consultatiedocument: http://www.ico.gov.uk/about_us/consultations/~/media/documents/consultation_responses/HMRC_consultation_implementing_UK-US_FATCA_Agreement_20120918.ashx.

Het uiteindelijke oordeel dat een land wel of geen passend beschermingsniveau blijkt te bieden, is aan de Europese Commissie (art. 25 lid 2 jo. art. 31 lid 2 Richtlijn).[116] Het Europees besluit daartoe wordt in ons land in een ministeriële regeling of een beschikking neergelegd (art. 78 lid 2 Wbp). Zolang er geen zodanige beslissing is genomen, bepaalt de verantwoordelijke zelf in eerste aanleg of het privacyniveau in het ontvangende land voldoende is.[117] De Europese Commissie had al vrij snel ten aanzien van Zwitserland en Hongarije een positieve beslissing genomen.[118] Sindsdien zijn er diverse landen gevolgd. Laatstelijk Nieuw Zeeland.[119]

Blijkt een derde land niet over een passend beschermingsniveau te beschikken, dan kan doorgifte onder bepaalde voorwaarden desalniettemin plaatsvinden. Art. 77 lid 1 Wbp noemt de betreffende voorwaarden, waaronder de ondubbelzinnige toestemming van de betrokkene of het voorhanden zijn van een overeenkomst tussen de betrokkene en de verantwoordelijke. Sinds 2012 kan ook bij het gebruik maken van door de Europese Commissie goedgekeurde modelcontracten doorgifte plaatsvinden vanuit Europa.[120] De Europese Commissie heeft twee modellen goedgekeurd. Een voor export naar een verantwoordelijke[121] en één voor uitbesteding aan een buitenlandse bewerker.[122]

Ook kan de minister, gehoord het College Bescherming Persoonsgegevens, een vergunning afgeven voor de export naar het betreffende land. Aan deze vergunning zullen veelal nadere voorschriften worden verbonden om de noodzakelijke bescherming van de persoonsgegevens te waarborgen (art. 77 lid 2 Wbp).

Grote internationale concerns hebben het probleem dat ze in ieder Europees land met de plaatselijke toezichthouder afspraken moeten maken over de export van persoonsgegevens naar derde landen. Aan deze bezwaren wordt tegemoet gekomen door middel van Binding Corporate Rules (BCR).[123] Het gaat om een intra groep privacypolicy die door drie Europese privacytoezichthouders moet worden goedgekeurd waarna interne doorgiften naar landen zonder adequate level of protection zijn toegestaan. De art. 29-werkgroep heeft diverse adviezen over BCR gepubliceerd.[124] De art. 29-werkgroep heeft in 2012 ook een model opgesteld speciaal ten behoeve van multinationale bewerkers.[125]

De doorgifte naar derde landen blijft een complexe aangelegenheid, reden waarom de Europese Commissie onder meer op 17 maart 2009 een zeer uitgebreide set van FAQ's publiceerde.[126]

Over het bereik van de artikelen 25 en 26 van de richtlijn (en daarmee art. 76 en 77 Wbp) heeft het Europese Hof in de Lindqvist-zaak een interessante uitspraak gedaan.[127] Naar de mening van het Europese Hof is *geen sprake is van doorgifte van gegevens naar een derde land in de zin van artikel 25 van richtlijn 95/46, wanneer een persoon in een lidstaat persoonsgegevens plaatst op een internetpagina bij zijn in dezelfde of in een andere lidstaat gevestigde hosting provider, en deze persoonsgegevens aldus toegankelijk maakt voor eenieder die een internetverbinding tot stand brengt, met inbegrip van personen die zich in derde landen bevinden*.[128]

Toepasselijk recht

In art. 4 Wbp wordt de kwestie van het toepasselijk recht geregeld. De Wbp kiest als aanknopingspunt voor jurisdictie de vestigingsplaats van de voor de verwerking verantwoordelijke. De formulering van artikel 4 is gebaseerd op artikel 4 van de richtlijn. Dat artikel wordt binnen de Europese Unie niet overal op dezelfde wijze

---

[116] Intussen wordt de verantwoordelijke zelf gedwongen tot een afweging omtrent het beschermingsniveau in het ontvangende land.

[117] *Handelingen I* 3 juli 2000, 34-1635.

[118] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304), OJ L215/1 of 25/08/2000; Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary, OJ L215/4 of 25/08/2000.

[119] Commission implementing decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand, Official Journal L 28/12, 30/1/2013.

[120] Zie Stb 2012, 33. Art. 77 lid 1 sub *g*.

[121] Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, L 385/74 EN Official Journal of the European Union 29.12.2004.

[122] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries, L 39/5 EN *Official Journal of the European Union* 12.2.201.

[123] Voor een uitgebreide beschrijving zie Lokke Moerel, *Binding Corporate Rules. Corporate Self-Regulation of Global Data Transfers*, Oxford: Oxford University Press 2012.

[124] Zie: WP 74, WP 108, WP 133, WP 153 en WP 155.

[125] Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP195 d.d. 6 June 2012. Zie vervolgens WP204 (Explanatory Document on the Processor Binding Corporate Rules, april 2013).

[126] Frequently Asked Questions relating to Transfers of Personal Data from the EU/EEA to Third Countries (http://ec.europa.eu)

[127] Prejudiciële zaak C101/01 (Bodil Lindqvist): zie overwegingen 52 t/m 71.

[128] Zie Winkelhorst en van der Linden Smith, *Persoonsgegevens op Intenet*, NJB 2004, p. 627. Zie ook Berkvens, *De Lindqvist case of de onbevlekte ontvangenis van persoonsgegevens*, Privacy & Informatie 2004/1.

uitgelegd en is ook in Nederland aanleiding geweest tot veel discussie.[129] De Wbp stelt dat de Nederlandse bepalingen worden toegepast, indien de verwerking van persoonsgegevens wordt verricht in het kader van de activiteiten van een vestiging van een verantwoordelijke in Nederland. Heeft de verwerker meerdere vestigingsplaatsen in de Europese Unie dan zal hij er zorg voor moeten dragen dat elk van de vestigingen aan de regels van het betreffende land van vestiging voldoet. Voor de vraag of sprake is van een *vestiging* is niet de rechtsvorm van de vestiging relevant (zowel een bijkantoor als een dochteronderneming worden als vestiging aangemerkt), maar is de concrete activiteit doorslaggevend.[130] Een en ander betekent dat ten aanzien van de verwerking van persoonsgegevens binnen één concern met dochterondernemingen in diverse lidstaten, meerdere nationale regelingen van toepassing zijn.[131] Deze situatie kan er – afhankelijk van de nationale invulling van eventuele aanmeldingsprocedures – toe leiden dat iedere vestiging in de betreffende lidstaat de verwerking zal moeten aanmelden.

Van het uitgangspunt dat de plaats van de gegevensverwerking niet relevant is voor jurisdictie is afgeweken in de situatie dat de verantwoordelijke verwerker niet op het grondgebied van een der lidstaten is gevestigd. In dit geval is onze nationale wet (Wbp) van toepassing indien voor de verwerking van persoonsgegevens gebruik wordt gemaakt van al dan niet geautomatiseerde middelen die zich op het grondgebied van Nederland bevinden, behalve indien deze middelen slechts voor de doorvoer van de persoonsgegevens worden gebruikt. De voor de verwerking verantwoordelijke moet ingevolge art. 4 lid 3 Wbp in Nederland een persoon of instantie aanwijzen die namens hem handelt overeenkomstig de bepalingen van de Wbp. Deze persoon of instantie wordt dan aangemerkt als zijnde de voor de verwerking verantwoordelijke. De reden voor opname van deze bepaling is dat op deze wijze een voor de verwerking van persoonsgegevens verantwoordelijke persoon of instantie zich niet door de keuze van een land van vestiging buiten de gemeenschap aan de jurisdictie van de in de gemeenschap gehanteerde bepalingen kan onttrekken. Het niet naleven van deze voorwaarde levert een strafbare handeling op (art. 75 Wbp).

Uit het bovenstaande blijkt dat ten aanzien van de vraag welk recht van toepassing is in eerste instantie wordt aangehaakt bij de vestigingsplaats van de voor de verwerking verantwoordelijke. Indien deze plaats zich buiten de gemeenschap bevindt, wordt aangeknoopt bij de plaats waar de verwerking plaatsvindt. De vestigingsplaats van de geregistreerde is niet van invloed.

Gegeven de grensoverschrijdende dimensie van het internet is de vraag interessant in hoeverre de Wbp van toepassing is op de diverse partijen die op het internet diensten verlenen. Conform art. 4 Wbp is de wet van toepassing op in het buitenland gevestigde internetaanbieders en transporteurs, indien ze gebruikmaken van geautomatiseerde middelen in Nederland. Wanneer deze middelen slechts worden gebruikt voor de doorvoer van persoonsgegevens sluit art. 4 lid 2 de Wbp echter weer van toepassing uit. Cruciaal is derhalve het antwoord op de vraag wanneer precies in het buitenland gevestigde internetaanbieders en transporteurs gebruikmaken van geautomatiseerde middelen in Nederland. Volgens Schreuders en Blok is dit afhankelijk van de vraag waar het verwerken van gegevens, waarvoor zij verantwoordelijk zijn, exact begint. Ter beantwoording van die vraag maken zij een onderscheid tussen passieve en actieve aanbieders en transporteurs. De verantwoordelijkheid van passieve partijen vangt aan zodra de gegevens, de pakketjes, bij hen arriveert. Immers, vanaf dat moment hebben zij de mogelijkheid om 'feitelijke macht' uit te oefenen. Passieve partijen zijn dus partijen die geen pakketjes naar de computer van de gebruikers sturen zonder een daaraan voorafgaand verzoek van die gebruiker. Ter illustratie laten we Schreuders en Blok zelf aan het woord: 'Stuurt een partij wel ongevraagd een pakketje naar de computer van de gebruiker met als doel op grond daarvan ook weer pakketjes terug te ontvangen, dan kan wellicht het zenden, maar zeker het terugontvangen van het 'gevraagde' pakketje worden beschouwd als het verzamelen van gegevens waarvoor deze partij verantwoordelijk is. Van deze vorm van verzamelen is in ieder geval sprake bij het gebruik van cookies en bij bijvoorbeeld een door de sitehouder verplicht gestelde inlogprocedure. In beide gevallen worden op grond van het enkele initiatief van de sitehouder pakketjes naar de computer van de gebruiker gezonden met als doel ook weer 'antwoord' terug te krijgen. Een actieve sitehouder of dienstenaanbieder verzamelt dus gegevens bij of op de computer van de gebruiker en maakt daarmee en daardoor dus gebruik van geautomatiseerde middelen die zich in Nederland bevinden. Kortom: voor een buiten het grondgebied van de EU gevestigde 'verantwoordelijke'

---

[129] Zie E.M.L. Moerel, *Back to basics: wanneer is de Wet bescherming persoonsgegevens van toepassing?*, Computerrecht 2008/61 met reactie van M.A.H. Fontein-Bijnsdorp in Computerrecht 2008/6 en naschrift van Moerel in Computerrecht 2008/6. Zie vervolg op de discussie: G-J Zwenne en G.C.J. Erents, *Reikwijdte Wbp, enige opmerkingen over de uitleg van art. 4, eerste lid, Wbp*, P&I 2009/2.

[130] De richtlijn stelt als criterium dat het moet gaan om het effectief en daadwerkelijk uitoefenen van activiteiten voor een onbepaalde periode (overweging 19 van de richtlijn). Betreft het een activiteit van tijdelijke aard, dan kan niet worden gesproken van een vestiging (HvJ EG, zaak 205/84, *Uur.* 1986, p. 3755, r.o. 21 en HvJ EG 10 mei 1995, *NJ* 1995, 703).

[131] De FEDMA heeft inmiddels een Europese gedragscode goedgekeurd gekregen. Daardoor is het binnen de marketing sector mogelijk geworden om binnen concernverbanden met één enkel systeem te werken.

die actief gebruik maakt van geautomatiseerde middelen in Nederland, is de Wbp van toepassing. Is die partij passief, dan is de Wbp niet van toepassing.'[132]

Van belang is ten slotte dat de wettelijke bepalingen de territorialiteitsregels inzake het strafrecht onverlet laten. Dit betekent dat waar bepaalde handelingen onder art. 75 Wbp strafbaar zijn gesteld, de art. 1-8 Sr in samenhang met art. 91 Sr van toepassing zijn. Concreet leidt dit tot de situatie dat wanneer via het internet door een Amerikaanse provider diensten worden aangeboden en deze provider persoonsgegevens van Nederlandse consumenten verzamelt zonder deze daarvan op de hoogte te stellen, hij naar Nederlands recht strafbaar is omdat het hier een gedraging betreft waarvan het gevolg zich in Nederland afspeelt. Zo ook zal een Nederlandse internetprovider (verantwoordelijke) naar Nederlands recht strafbaar zijn indien hij in het buitenland onopgemerkt persoonsgegevens verzamelt.[133]

Evaluatie Wbp

Sinds de inwerkingtreding heeft de Wbp diverse kleinere technische aanpassingen ondergaan. Ultimo 2009 passeerde een omvangrijker pakket aanpassingen de Tweede Kamer met daarin onder meer aanpassingen van de regels voor gegevensexport, voorafgaand onderzoek en direct marketing.[134] Deze voorstellen zijn inmiddels in werking getreden.[135] Tevens werden bij die gelegenheid voorstellen aan de Tweede Kamer aangeboden gericht op uitbreiding van het vrijstellingen regime voor meldingen. Het vrijstellingsbesluit is inmiddels gewijzigd.[136] De Wbp bevat in artikel 80 een evaluatieverplichting. Inmiddels is Wbp inderdaad geëvalueerd.[137] Daarnaast is door de ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties een Adviescommissie ingesteld met als taak te rapporteren over het thema "veiligheid en persoonlijke levenssfeer".[138] Eind oktober 2009 verscheen de kabinetsreactie op de bevindingen van de twee evaluatierapporten en het rapport van de Adviescommissie (dat 10 maanden eerder was verschenen).[139] April 2011 publiceerde het Kabinet Rutte I een "privacy-agenda" [140], maar de nationale plannen en ambities om de Wbp bij de tijd te brengen, hebben inmiddels aan betekenis ingeboet door de Europese ontwikkelingen rond een privacyverordening.

Vooruitblik op Verordening[141]

Op 25 januari 2012 publiceerde de Europese Commissie een voorstel voor een Verordening, die Richtlijn 95/46 moet vervangen. [142] De keuze voor het instrument van de Verordening betekent dat de nieuwe regels directe werking binnen de lid-staten zullen hebben, waarmee aan de huidige variëteit aan interpretaties van Europese privacyregelgeving een einde moet komen. Vanaf het moment dat de Verordening van kracht wordt is het nieuwe regime van toepassing op zowel verantwoordelijken die een vestiging hebben in de EU als verantwoordelijken die daar niet zijn gevestigd, maar wel persoonsgegevens van EU-onderdanen verwerken. De verwachting is dat de discussie over het voorstel van de Commissie enige tijd in beslag zal nemen. Begin 2013 kwam de rapporteur voor het Europees Parlement, Albrecht, met een flink pakket aan aanvullende wensen.[143]

---

[132] E. Schreuders & P. Blok, 'Privacy en de WBP op het Internet', in: J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, 2e druk, Deventer 2000, p. 401-423.

[133] Vergelijk *Kamerstukken II*, 1997/98, 25 892, nr. 3, p. 193.

[134] *Kamerstukken II*, 2009/10, 31841, Voorstel tot aanpassing in het kader van de bestrijding van administratieve lasten.

[135] *Zie: Stb*. 2012, 33.

[136] *Zie: Stb*. 2012, 33.

[137] Zwenne, G-J e.a., Eerste fase evaluatie Wet bescherming persoonsgegevens, Litteratuuronderzoek en knelpuntenanalyse, WODC 2007; Winter, H.B. e.a., Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk, Groningen, 2009.

[138] Adviescommissie Veiligheid en persoonlijke levenssfeer (commissie Brouwer-Korf), *Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer*, Den Haag, 22-01-2009.

[139] *Kamerstukken II*, 2009/10, 31051, nr. 5. Voor een kritische bespreking: Buitelaar J.C. Cuijpers C.M.K.C. "De balans tussen veiligheid en privacy. Kanttekeningen bij het standpunt van het kabinet ", NJB 2009, p. 2194.

[140] *Kamerstukken II*, 2010/11, 32761, nr. 1.

[141] Zie in meer detail: het themanummer "Hervorming Europese gegevensbeschermingsregels" van het tijdschrift *Privacy & Informatie* voor diverse achtergrondartikelen over de nieuwe Europese regels, nr. 3 2012; H. Hijmans, "Nieuwe Europese regels voor privacy. Commissie stelt pakket voor om gegevens ook in het informatietijdperk te beschermen", *Nederlands Tijdschrift voor Europees Recht*, afl. 4 2012; C. Kuner, '*The European Commission's Proposed Data Protection Regulation:'A Copernican Revolution in European Data Protection Law'*,Privacy & Security Law Report, 11 PVLR 06, 02/06/2012.

[142] P*roposal COM(2012)11 Final for a regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*.

[143] Zie hierover: C. Burton, Ch. Kuner,A. Pateraki, "The Proposed EU Data Protection Regulation One Year Later: The Albrecht Report", *Privacy and Security Law Report* January 2013.

Ten tijde van de afsluiting van deze tekst, begin oktober 2013, bereikten de ministers van justitie op diverse punten overeenstemming en werd een eerste oriënterende stemronde in het Europees Parlement verwacht.

In vergelijking met Richtlijn 95/46 wordt de positie van betrokkenen versterkt via onder meer een aangescherpt regime voor toestemming, het recht om vergeten te worden en het recht op dataportabiliteit. Het recht om vergeten te worden verlangt van verantwoordelijken dat ze, onder bepaalde voorwaarden, op een verzoek daartoe van een betrokkene onmiddellijk tot de verwijdering van alle persoonsgegevens overgaan. Daarbij moet de verantwoordelijke er tevens voor zorgen dat derden aan wie de gegevens zijn verstrekt, deze gegevens eveneens verwijderen. Het recht op dataportabiliteit biedt betrokkenen de mogelijkheid om een afschrift van de over hen opgeslagen persoonsgegevens te krijgen, zodat zij deze gegevens over kunnen dragen aan organisatie of bedrijf waarmee ze een nieuwe relatie aangaan. Belangrijk is verder dat betrokkenen het recht krijgen toestemming te onthouden aan profilingactiviteiten, tenzij deze vorm van verwerking noodzakelijk is vanuit technisch oogpunt..

Het vereiste van toestemming is de afgelopen jaren een complexe kwestie gebleken.[144] Wat de vraag blijft onder welke omstandigheden nu wel of juist geen toestemming door de betrokkene is verleend voor het verwerken van zijn persoonsgegevens. De Commissie maakt in het voorstel voor de Verordening duidelijk dat wanneer de uitdrukkelijke toestemming van de betrokkene noodzakelijk is, toestemming alleen verkregen is als deze betrokkene expliciet zijn of haar wil heeft geuit. Dat betekent dat een stilzwijgende of impliciete toestemming onvoldoende zal zijn als grondslag voor de verwerking. In de gevallen dat ondubbelzinnige toestemming geldt wordt verlangd, betekent het dat er geen twijfel kan bestaan over de vraag of de betrokkene toestemming heeft gegeven en voor welke specifieke verwerkingen die is gegeven. Bij dit alles ligt de bewijslast bij de verantwoordelijke. Nieuw is verder dat een verantwoordelijke aan de betrokkenen moet laten weten gedurende welke periode de persoonsgegevens worden opgeslagen. Een belangrijke pijler van de Verordening is het vereiste van *accountability*: van verantwoordelijken wordt verlangd dat hij zeker stelt dat de bepalingen van de Verordening worden nageleefd en dit ook valt aan te tonen. Concreet betekent dit vereiste dat verantwoordelijken veel meer dan nu het geval is moeten protocolleren en documenteren wat ze met persoonsgegevens doen. Met andere woorden, het opstellen van beleidsregels en nemen van maatregelen om *compliance* van het voorwaarde te garanderen zal van verantwoordelijken het nodige gaan vragen. Daarbij komt dat zij ook nog aan diverse andere verplichtingen zullen moeten gaan voldoen, zoals de plicht om datalekken binnen 24 uur te melden en - voor bedrijven met meer dan 250 werknemers - een privacyfunctionaris aan te stellen. Dat een en ander kosten met zich mee gaat brengen is een ding dat zeker is.[145] Tenslotte moet nog worden gewezen op het voorstel om bewerkers, onafhankelijk van contractuele afspraken die ze met een verantwoordelijke maken, ook verantwoordelijk te laten zijn voor de gegevensbeveiliging.

Tegenover deze aanscherping van de voorwaarden staat een vereenvoudiging van de regels voor grensoverschrijdend persoonsgegevensverkeer naar landen buiten de EU. Verantwoordelijken met meerdere vestigingen in Europa zullen in de toekomst alleen nog maar te maken hebben met de toezichthouder van het land waar hun hoofdvestiging is (zgn. one-stop-shop). Verder zal bij het gebruik van een Europees modelcontract of Binding Corporate Rules niet langer een exportvergunning vereist zijn. Ook contractuele afspraken kunnen in principe volstaan als een voldoende waarborg voor bescherming in het geval van export van gegevens, maar alleen op voorwaarde van toestemming door de nationale toezichthouder.

3. Conclusie

Waar het onderwerp ‘bescherming van persoonsgegevens’ ten tijde van de eerste druk van deze bundel nog primair een onderwerp van academisch debat was, hebben de ontwikkelingen de afgelopen jaren een enorme vlucht genomen. ‘Privacy’ is inmiddels een thema dat op de agenda van vrijwel iedere ICT-jurist staat. Met de komst van de nieuwe Europese regels zal dat de komende jaren niet anders zijn. Deze bijdrage stond in zeer kort bestek stil bij het regime van de huidige Wbp en de belangrijkste wijzigingen die er met de Europese Verordening aankomen. Wie (veel) meer wil weten, wende zich tot de overvloed aan literatuur, online discussiefora en congressen over dit onderwerp.

---

144 Zie onder meer E. Kosta, *Consent in European Data Protection Law*, Nijhoff Studies in European Union Law, Martinus Nijhoff Publishers 2013.

145 P.M.H.H. Bex, M.A. Bloemheuvel, S.A. Prij, *Toetsing Europese Dataprotectieverordening* , Sira Consulting, Nieuwegein mei 2013; *Kamerstukken II*, 2012/13, 32 761, nr. 50. (aanbieding rapport aan TK).

Geraadpleegde en aanbevolen literatuur

Adviescommissie Veiligheid en persoonlijke levenssfeer (commissie Brouwer-Korf), *Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer*, 22-01-2009.

Alberdingk Thijm, C., *Privacy vs. Auteursrecht in een digitale omgeving*, ITeR-serie nr. 49, Den Haag: Sdu 2001.

Bennet, C.J. & Ch.D. Raab, 'The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response', *The Information Society* 13.

Berkvens, J.M.A., 'Het goede doel', *Privacy en informatie* 2001, nr. 2.

Bitter, C.M., "Privacyprocesrecht," in: J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, 4e druk, Deventer 2007.

Blas, D.A., 'Towards a uniform application of the European Data Protection Rules, The role of the Article 29 Working Party', *Privacy & Informatie* 2001/1.

Blok, P. & A. Vedder, 'Privacy in ontwikkeling', in: J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, 3e druk, Deventer 2002.

Blok, P., *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*, Meppel: Boom Juridische Uitgevers, 2002.

Borking, J, *Privacyrecht is code, over het gebruik van privacy enhancing technologies* (diss: Leiden RUL), Wassenaar: 2010.

Brouwer, J.G., *Compendium Wet bescherming persoonsgegevens, tekst en toelichting*, Den Haag: Koninklijke Vermande, 2002.

Cuijpers, C., P. van der Putt, J. Terstegge, *Privacy Concerns. Het delen van persoonsgegevens bij fusies, overnames en binnen concerns*, NVvIR preadvies, Elsevier juridisch 2003.

Cuijpers, C., *Privacyrecht of privaatrecht? Een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn*, Iter-reeks nr. 71, SDU, Den Haag 2004 (diss.).

De gewaardeerde klant, serie Achtergrondstudies en Verkenningen nr. 18, Den Haag: Registratiekamer, september 2000.

Dijk, van e.a. (red.), *Uitsprakenbundel Wet bescherming persoonsgegevens*, Den Haag, SDU 2009.

Ebbers, C.W.J.M., A.C.M. de Heij, P.J.D.J. Muijden, J.E.J. Prins (red.), *Voorschriften Privacybescherming*, Deel C, Den Haag: Elsevier.

Esch, R.E. van, Blok, P, 'Privacy en elektronische handel via internet' in: J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, 4e druk, Deventer 2007.

FTC, 'Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress', May 2000.

Gutwirth, S. e.a., Reinventig Data Protection, Springer Science+Business Media B.V., 2009.

Hoboken, J.V.J. van en A.M. Arnbak , N.A.N.M. van Eijk, m.m.v. N. Kruijssen, ' Cloud diensten in hoger onderwijs en onderzoek en de USA Patriot Act', *Instituut voor Informatierecht* (UVA), Amsterdam: september 2012.

Holvast, J., *Het gebruik van persoonlijkheidsprofielen in de publieke sector*, ITeR-serie 42, Den Haag: Sdu, 2001.

Holvast, *De volkstelling van 1971*, Zutphen: Uitgeverij Paris 2013.

Hooghiemstra, T.E.M. en Nouwt, S., *SDU Commentaar Wet bescherming persoonsgegevens*, Den Haag: SDU 2e druk 2011.

Hooghiemstra T.F.M. e.a.(red), *Jurisprudentie Bescherming Persoonsgegevens*, Den Haag: SDU uitgevers, 2013.

Huydecoper S.M., *Wet bescherming persoonsgegevens en ICT*, Den Haag: Sdu 2006 (Mongrafieen Recht en Informatietechnologie deel 4).

Klant in het Web, serie Achtergrondstudies en Verkenningen nr. 17, Den Haag: Registratiekamer, juni 2000.

Knol P.C. & Zwenne G.J. (red), *Tekst & Commentaar Telecommunicatie- en privacyrecht*, Deventer: Kluwer 2013 (vierde druk).

Koëter, J, *Behavioral Targeting en privacy, een juridische verkenning van internet gedragsmarketing*, Tijdschrift voor internetrecht, 2009/4.

Koops, E.J., A. Vedder, *Opsporing versus privacy: de beleving van burgers*, ITeR-serie 45, Den Haag: Sdu uitgevers, 2001.

Kranenborg H.R., Verhey L.F.M., *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Kluwer 2011.

Kranenborg H.R., "Nieuwe Europese regels voor de bescherming van persoonsgegevens: van belang voor iedereen", *SEW* 2013, nr. 7/8.

Kuitenbrouwer F., 'Privacy: een historisch-vergelijkend overzicht', in: J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, 3e druk, Deventer 2002.

Kuner, C., European data privacy law and online business, New York: Oxford University Press 2003.

Kuner, C., '*The European Commission's Proposed Data Protection Regulation:'A Copernican Revolution in European Data Protection Law'*,Privacy & Security Law Report, 11 PVLR 06, 02/06/2012.

Kuner, C. *Transborder Data Flow Regulation in Data Protection and Privacy Law*, diss. Universiteit Tilburg 2012.

Moerel, L, *Binding Corporate Rules, Fixing the regulatory patchwork of data protection* (diss. Tilburg, UVT) Amsterdam: 2011.

Overkleeft-Verburg, G., *De Wet Persoonsregistraties. Norm, toepassing en evaluatie*, Zwolle 1995.

Prins, J.E.J. & J.M.A. Berkvens, 'De Wet bescherming persoonsgegevens', in: J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, 4e druk, Deventer 2007.

Prins J.E.J., "Acht gesprekken over privacy en aanpalende belangen", *Zeven essays over informatietechnologie en recht*, ITeR-serie nr. 63, Den Haag: Sdu Uitgevers, 2003.

Prins J.E.J., "Technocratie en de toekomstagenda van de Nationale Ombudsman", in: *Werken aan behoorlijkheid. De Nationale Ombudsman in zijn context* (jubileumbundel 25 jaar Nationale Ombudsman), Den Haag: Boom Juridische Uitgevers 2007, pp. 111-134.

Prins J.E.J., "De eOverheid voorbij: Recht doen aan de digitale werkelijkheid", *Preadvies voor de VAR Vereniging voor Bestuursrecht*, Boom Juridische Uitgevers 2011, pp. 71-116.

Prins J.E.J., "De klank van veiligheid", Nederlands Juristenblad, 2013, p. 1489.

Sauerwijn, L.B. en Linneman, J.J., *Handleiding voor verwerkers van persoonsgegevens*, brochure Ministerie van Justitie versie 13-7-2006.

Schreuders, E. & P. Blok, 'Privacyregels en de Wbp op het Internet', in: J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, 3e druk, Deventer 2002.

Tempelman, J.A., *Nieuwe regels met betrekking tot spam en telemarketing*, Tijdschrift voor consumentenrecht en handelspraktijken, 2009/5.

Terstegge, J, 'Internationaal gegevensverkeer', in: J.E.J. Prins & J.M.A. Berkvens (red.), *Privacyregulering in theorie en praktijk*, 4e druk, Deventer 2007.

Terstegge, J.H.J., 'Van de regen en de drup', *Nederlands Tijdschrift voor Bestuursrecht, nr. 2000/8 p. 243 e.v.*

Terstegge, J.H.J., *De wet bescherming persoonsgegevens. Handleiding voor de praktijk. Dossier*, Alphen aan den Rijn/Zaventem: Samsom 2000.

Terstegge, J.H.J., H.H. de Vries, T.A.J. Reinders, I. van der Helm, *Wet bescherming persoonsgegevens*. Deventer: Kluwer 2001.

Thole, E., "*e*-Privacyrichtlijn maakt geen eind aan spam", *NJB* afl. 4, 23 januari 2004, pp. 168-173.

Thijssen, M.B.J., *De Wbp en de vennootschap*, Serie Recht en Praktijk 171, Kluwer: Deventer, 2009.

Vedder, A., 'Het einde van de individualiteit?: datamining, groepsprofilering en de vermeerdering van brute pech of dom geluk', *Privacy & Informatie* 1998/3.

E. Verhelst, *Recht doen aan privacyverklaringen* (diss: Tilburg UVT), Tilburg: 2012.

Viergever, L en Koëter, J., 'Is onze privacyregelgeving "Big data proof?"', *Tijdschrift voor Internetrecht*, 2012, nr. 6.

Winter, H.B. e.a., *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*, Groningen, 2009.

Wbp-naslag, http://www.cbpweb.nl/wbpnaslag/.

Zwenne, G-J e.a., *Eerste fase evaluatie Wet bescherming persoonsgegevens, Litteratuuronderzoek en knelpuntenanalyse*, WODC 2007.